AmeriCorps

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2022 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF AMERICORPS

FINAL AUDIT REPORT

NUMBER: OIG-EV-23-03

April 3, 2023

OFFICE OF INSPECTOR GENERAL
AmeriCorps

OFFICE OF INSPECTOR GENERAL
AmeriCorps

April 3, 2023

MEMORANDUM TO:	Syed Murshed Acting Chief Information Officer
FROM:	Monique P. Colter Monique P. Colter Assistant Inspector General for Audit
SUBJECT:	Fiscal Year 2022 Federal Information Security Modernization Act Evaluation of AmeriCorps (OIG Report- EV-23-03)

Enclosed is AmeriCorps Office of Inspector General (OIG) final report on the Fiscal Year 2022 Federal Information Security Modernization Act (FISMA) Evaluation of AmeriCorps, OIG Report EV-23-03.

The OIG contracted with the independent certified public accounting firm of RMA Associates, LLC (RMA) to conduct the FISMA evaluation for Fiscal Year (FY) 2022. 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 final 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
Bilal Razzaq, Chief Information Security Officer
Fernando Laguarda, General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits and Investigations Program Manager
Deborah Jeffrey, 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 2022

March 31, 2023

Table of Contents

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) 2022.

The objective of this evaluation was to determine the effectiveness of AmeriCorps' information security program and practices for the period October 1, 2021, through September 30, 2022, and report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. This report presents the results of RMA's independent evaluation of AmeriCorps information security program and practices.

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

Key Changes to the FY 2022 IG FISMA Metrics

As part of our evaluation, we responded to the fiscal year FY 2022 Core Inspector General Metrics (FY 2022 Core IG Metrics) specified in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (issued on April 13, 2022). We also considered applicable OMB policy and guidelines and the National Institute of Standards and Technology (NIST) standards. These core metrics provide reporting requirements across the five functional areas within the FISMA maturity model to be addressed in the independent assessment of agencies' information security programs.[2] See Objective, Scope, and Methodology for more detail.

OMB encourages agencies to adopt a continuous evaluation approach for independent assessments. OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) have revised the reporting metrics to support this shift to cover multiple years. This change has involved reducing the number of metrics from 66 to 20, based on the FY 2021 IG FISMA Reporting Metrics v1.1 (May 2021). The FY 2022 Core IG Metrics have been chosen to align with Executive Order (EO) 14028 (May 12, 2021), which aims to enhance national cybersecurity and recent OMB guidelines for modernizing federal cybersecurity. The 20 core metrics, including key Administration goals and essential controls, will be evaluated annually, while the remaining metrics, known as supplemental metrics, will be evaluated biennially.

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (December 18, 2014).
[2] The FY 2022 IG FISMA Reporting Metrics align with the five functional areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework [CSF]), version 1.1: Identify, Protect, Detect, Respond, and Recover.

Summary Evaluation Results

We found that AmeriCorps' information security program and practices were **not effective** for the period October 1, 2021, through September 30, 2022. Within the context of the FISMA maturity model, an effective level of security is *Managed and Measurable* (Level 4). We assessed AmeriCorps' information security program overall maturity level at *Defined* (Level 2), as described in this report.

Overall, AmeriCorps made little progress in maturing its information security program from FY 2018 to FY 2022. From FY 2018 to FY 2021, maturity metrics remain unchanged. This year, AmeriCorps advanced in one function area: Recover. Table 1 depicts AmeriCorps' maturity levels by security functions between FY 2018 to FY 2022.[3]

Table 1: Comparison of Maturity Ratings by Function in FYs 2018 – 2022

Security Function[4]	Maturity Level FY 2018	Maturity Level FY 2019	Maturity Level FY 2020	Maturity Level FY 2021	Maturity Level FY 2022[5]
Identify	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Protect	Defined[6] (Level 2)	Defined[7] (Level 2) – *Assessed Rating*[8]	Defined[9] (Level 2)	Defined[10] (Level 2)	Defined[11] (Level 2)
Detect	Defined (Level 2)	Ad Hoc (Level 1)	Ad Hoc (Level 1)	Defined (Level 2)	Defined (Level 2)
Respond	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)

[3] FY 2022 evaluation was based on 20 core metrics from the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines.* In FY 2021, the evaluation was based on 66 metrics.

[4] See Appendix I Table 11 and Table 12 for definitions and explanations of the Cybersecurity Framework Security Functions (CSF) and Metric Domains.

[5] FY 2022 evaluation was based on 20 core metrics from the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines.*

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

[7] Ibid 6.

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

[9] Ibid 6.

[10] Ibid 6.

[11] Ibid 6.

Security Function[4]	Maturity Level FY 2018	Maturity Level FY 2019	Maturity Level FY 2020	Maturity Level FY 2021	Maturity Level FY 2022[5]
Recover	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)
Overall	**Not Effective**	**Not Effective**	**Not Effective**	**Not Effective**	**Not Effective**

Consistent implementation of an information security program and monitoring security controls remains a challenge for AmeriCorps. The agency developed an overall strategy for improving IT security to an effective level and created an accountability structure necessary to achieve that result. However, it did not fully implement that strategy. The effectiveness of the strategy cannot be evaluated at this time.

AmeriCorps also did not make significant progress in implementing prior recommendations, some dating back to 2017. Since last year, the agency took actions to resolve 12 of 30 open recommendations from the FY 2017 – FY 2021 FISMA evaluations, yielding slight improvements in IG FISMA Metrics results. Implementing more of these recommendations will help AmeriCorps mature its information security program and increase its effectiveness. We issued three new recommendations in FY 2022. See Appendix III for the status of prior year recommendations.

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

- Mobile Devices;
- IT asset inventory management;
- Vulnerability and patch management program;
- Personal Identify Verification (PIV) multifactor authentication (MFA);
- Performance measures;
- Security Assessments; and
- Contingency planning.

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

1. The **Identify** function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities. For FY 2022, the Identify function remains at *Defined* (Level 2) because AmeriCorps did not fully implement the organization-wide risk management strategy, and control weaknesses remain with mobile device management and IT asset inventory.

   AmeriCorps improved the risk management strategy by creating a Tier 2 risk register. However, additional time for implementation and more testing is needed to determine the risk register's effectiveness. AmeriCorps can increase the maturity level of this function by properly managing the IT asset inventory and fully implementing mobile device management.

AmeriCorps needs to fully implement controls over its mobile devices. Its Mobile Device Management (MDM) software did not protect all its mobile devices. Also, of those mobile devices covered by the MDM, it has yet to implement security features that prevent the execution of unauthorized software.

AmeriCorps has incomplete inventory records of hardware assets connected to the network. In addition, AmeriCorps did not consistently use its standard elements/taxonomy to develop and maintain an inventory of hardware assets in accordance with AmeriCorps policies and procedures.

2. The **Protect** function outlines appropriate safeguards to ensure the delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event. AmeriCorps' Protect function also remains at the *Defined* (Level 2) maturity level this year because of the issues related to PIV MFA and vulnerability management.

PIV MFA continues to be an issue for AmeriCorps. Although AmeriCorps planned to use strong authentication mechanisms for privileged users[12] of AmeriCorps' facilities, systems, and networks, we noted that MFA was not consistently implemented, nor did it provide information regarding implementing their cyber security policy on using PIV cards. MFA was not implemented because the majority of the AmeriCorps' workforce continued to telework during FY 2022 due to the COVID-19 pandemic.

Vulnerability and patch management controls were not consistently employed. Specifically, critical and high-risk vulnerabilities were not resolved within the timeframes specified by its internal operating policies. As a result, vulnerabilities related to patch management, configuration management, and unsupported software continue to expose AmeriCorps' network to critical and high-severity vulnerabilities. These control weaknesses affected five of the eight metrics in this domain.

AmeriCorps did not use qualitative and quantitative performance metrics to measure, report, and monitor the information security performance of its data exfiltration and enhanced network defenses, incidence detection and analysis process; and incidence handling process.

The most effective way for AmeriCorps to improve its maturity level in the Protect function is to reinstate mandatory enforcement of PIV MFA, implement performance measures, and strengthen vulnerability and patch management controls.

[12] A privileged user is a user authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. A non-privileged user is an ordinary user who is authorized to access an information system.

3. The **Detect** function, which defines the appropriate activities to identify the occurrence of a cybersecurity event, remained at the *Defined* (Level 2) maturity level because AmeriCorps did not consistently conduct annual security assessments and prepare Security Assessment Reports for all information systems in line with its policies and procedures.

4. The **Respond** function, which includes appropriate activities to support the ability to contain the impact of a potential cybersecurity incident, remained *Consistently Implemented* (Level 3) and, therefore, not effective.

5. Lastly, the **Recover** function, which includes activities to support timely recovery to normal operations to reduce the impact of a cybersecurity incident, improved this year to an effective rating, *Managed and Measurable* (Level 4). However, AmeriCorps did not update its Continuity of Operations Plan (COOP) as part of its annual review process. The plan review and revisions were overdue for 16 months until the new COOP was signed on July 14, 2022.

Focusing on the controls assessed as *Defined* (Level 2) is key for AmeriCorps to increase function areas to an effective maturity level. To address the continuing weaknesses in AmeriCorps' information security program and practices, we added three new recommendations to the 30 unimplemented recommendations from prior years. Implementing these recommendations will assist AmeriCorps in addressing challenges in developing a mature and effective information security program.

Management's Response and Evaluator's Comments

AmeriCorps concurred with all findings and recommendations. AmeriCorps stated that it is committed to continuously strengthening its cybersecurity posture and considers cybersecurity a critical focus area. AmeriCorps noted the OIG findings and recommendations added value and were risk-based. AmeriCorps indicated that it invested an additional $1.7 million into its Cybersecurity Program in FY22 and has made significant changes, including process improvements, the execution of an Interconnection Security Agreement with the Social Security Administration, and enhancement of Security Impact Analysis procedures. AmeriCorps will continue to focus on improving its cybersecurity management functions, particularly in areas such as multifactor authentication, vulnerability and patch management controls, and annual security assessment processes. We will evaluate AmeriCorps' corrective actions addressing current and prior year recommendations in the FY 23 FISMA evaluation.

AmeriCorps' comments are included in their entirety in Appendix IV. Our evaluation of AmeriCorps' comments is included in Appendix V.

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

RMA Associates

Arlington, VA
March 31, 2023

FISMA Evaluation Findings

Security Function: Identify

1. AmeriCorps Must Centrally Manage All Agency Mobile Devices and Complete Migration to the New MDM System

FY 2022 IG FISMA Function: *Identify* / **Domain**: *Risk Management*

Mobile devices often need additional protection because their nature generally places them at higher threat exposure than other devices. For this reason, AmeriCorps centrally manages its mobile devices through an enterprise-wide MDM system. An enterprise-wide MDM system is essential because it can provide consistent management, configuration, security, and continuous monitoring of all AmeriCorps mobile devices.

AmeriCorps changed its MDM tool, Maas360, to the Microsoft Intune tool, which provides more stringent controls. The transfer is a time-consuming manual process requiring users to travel to AmeriCorps headquarters. As a result of the transfer, AmeriCorps indicated that 43 percent of its mobile devices were not managed by an MDM tool. Also, of the 57 percent covered by the MDM, the security features to prevent the execution of unauthorized software were not implemented.

NIST requires AmeriCorps to establish the configuration standards[13] of all mobile devices connected to its networks, including mobile devices under its control and those mobile devices not under its control. In addition, NIST requires mobile device security[14] to:

- Limit or prevent access to AmeriCorps services based on the mobile device’s operating system version and restrict installing applications through whitelisting (preferable) or blacklisting.
- Install security and operating system updates within a prescribed period or deny access to enterprise services by devices not updated within that prescribed period; and
- Implement a process to prevent users from installing/downloading unauthorized software on their official mobile devices.

Without technical controls preventing the installation of potentially harmful software on AmeriCorps mobile devices, employees can introduce, both purposefully and inadvertently, potentially dangerous software and malware into the AmeriCorps computing environment. In addition, without specifying how quickly users must apply available security and operating system updates and without an automated tool to validate and enforce compliance, AmeriCorps’ mobile devices remain vulnerable to potential security threats.

[13] NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, control AC-19, Information System Component Inventory, Pages 51-52.
[14] NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Page 8.

The FY 2020 FISMA evaluation report[15] recommended that AmeriCorps implement a process to (1) deny access to AmeriCorps enterprise services for mobile devices that have not been updated within the prescribed period and (2) block unauthorized applications from installing on AmeriCorps mobile devices. Management did not implement these recommendations, and therefore, FY 2020 Recommendations 2 and 3 remain open. We are not issuing a new recommendation.

2. AmeriCorps Must Improve Its Inventory Management Process

FY 2022 IG FISMA Function: *Identify* / **Domain**: *Risk Management*

Managing IT inventory is foundational to effective cybersecurity. Maintaining accurate and reliable inventory data is necessary for managers to make effective budgeting, operating, and financial decisions. Proper inventory accountability requires the maintaining of detailed inventory records and reporting in the entity's IT and financial management records and reports. Federal agencies are required to develop and document an inventory of information system components that: (1) accurately reflects the current information system and (2) includes all components within the authorization boundary of the information system.[16] In addition, the agency's internal policy, entitled *AmeriCorps Cybersecurity Control Families*, requires the information system component inventory to be reviewed and updated at least annually.

AmeriCorps did not maintain an up-to-date inventory of hardware assets connected to the network. Specifically, the total population of 3,310 IT assets on the inventory listing were missing the list of required fields.

The primary user was not documented for 258 assets; 216 were laptops, workstations, printers, servers, IP Phones, Firewalls, Office of Information Technology (OIT) Equipment, and OIT Networking gear. Specifically, in FY 2022:

- Serial numbers were not documented for 40 assets; and
- Asset numbers were not documented for 176 assets.

Table 2 shows AmeriCorps' limited progress in controlling its hardware inventory from the prior year.

Table 2: Hardware Assets Comparison

Description	FY 2022	FY 2021
Inventory Of Hardware Assets	3,310	3,436
No Documentation of the Primary User	258	279

[15] Recommendations 3, *Fiscal Year 2001 Federal Information Security Modernization Act Evaluation of AmeriCorps*, OIG Report Number OIG-EV-21-03 (December 18, 2020), Page 6.

[16] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, control CM-8, Information System Component Inventory, Pages 107-108.

Description	FY 2022	FY 2021
No Serial Numbers	40	61
No Asset Numbers	176	91

In addition, AmeriCorps did not update all the fields when moving items in and out of storage at the AmeriCorps Headquarters as specified in *AmeriCorps SOP Asset Tracking Procedures*, Version 2. Also, AmeriCorps did not implement a spot check to ensure they followed the established procedures to remedy this issue based on the prior year's recommendation. Furthermore, the Tier 2 Support Lead did not provide refresher training on the Asset Tracking Procedures.

There are significant ramifications for an organization that fails to maintain accurate and reliable inventory data. Incomplete or inaccurate inventories could result in a loss of confidentiality, misappropriation, and waste. Stolen or misplaced computing equipment could put AmeriCorps at risk of losing control of their data and equipment. This may also cause a strain on the AmeriCorps budget as unplanned and unnecessary spending may be required to replace stolen or misplaced computing equipment.

Management did not implement recommendations 2 and 3 from the FY 2021 FISMA evaluation report[17] to complete asset tracking refresher training for Tier 2 support and update and implement the *AmeriCorps SOP Asset Tracking Procedures*. The asset tracking procedures must include a quality control process for reviewing the IT asset inventory and ensuring the required fields for the IT assets were documented. Therefore, these recommendations remain open. We are not issuing a new recommendation.

[17] Recommendations 2 and 3, *Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of AmeriCorps*, OIG Report Number OIG-EV-22-03 (December 15, 2021), Page 9.

Maturity Model Scoring

The maturity level based on the six IG FISMA Metrics for the "Identify" function is Level 2 (*Defined*), Not Effective, as depicted in Table 3.[18]

Table 3: Security Function Identify Metrics

Maturity Level	Count	IG FISMA Metrics
Ad Hoc (Level 1)	1	14
Defined (Level 2)	3	2, 5, and 10
Consistently Implemented (Level 3)	1	3
Managed and Measurable (Level 4)	1	1
Optimized (Level 5)	-	N/A
Calculated Maturity Level: Defined (Level 2), Not Effective		

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

Security Function: Protect

3. AmeriCorps Must Improve its Vulnerability and Patch Management Controls

FY 2022 IG FISMA Function: *Protect* / **Domain**: *Configuration Management*

Patch management is identifying, acquiring, installing, and verifying patches for products and systems and is an important component of vulnerability management. Protecting government computer systems has never been more important because of the complexity and interconnectivity of systems (including Internet and wireless), the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. We conducted scans for known vulnerabilities (patch levels, legacy operating systems, and host configurations). AmeriCorps provided 1,202 Internet Protocol (IP) addresses for RMA to scan for vulnerabilities.

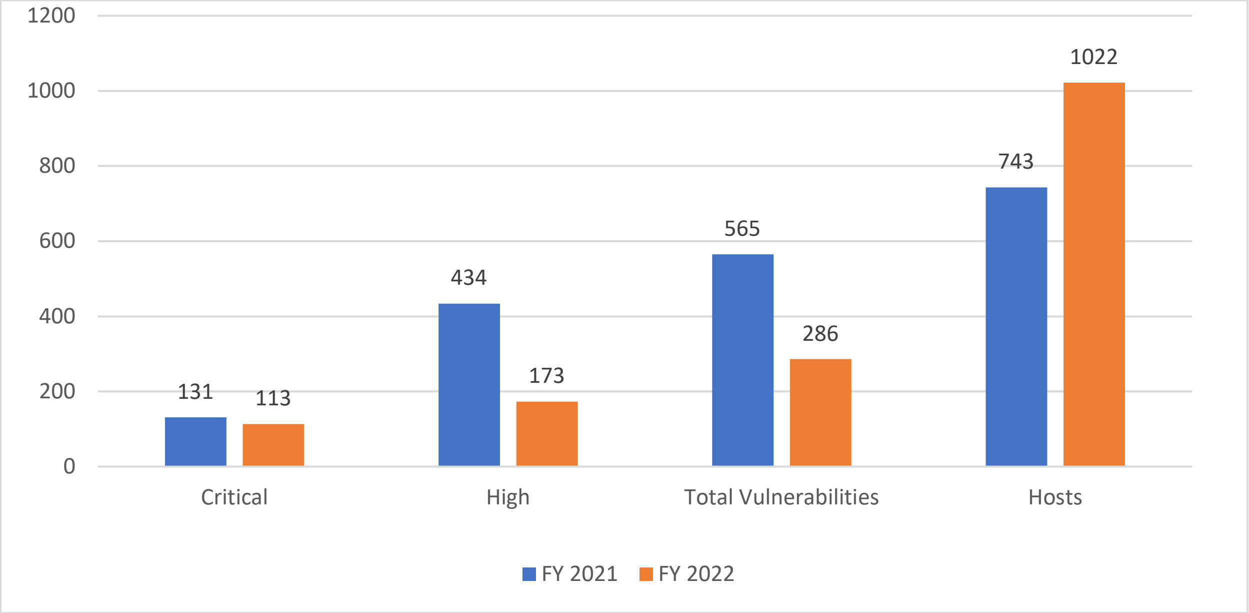
Critical and High Vulnerabilities

AmeriCorps has improved its vulnerability management program from prior years by reducing the amount of critical and high vulnerabilities. Specifically, AmeriCorps decreased Critical vulnerabilities from 131 in FY 2021 to 113 in FY 2022 and decreased High vulnerabilities from 434 in FY 2021 to 173 in FY 2022. Also, during FY 2022, AmeriCorps decreased the percentage of hosts affected by vulnerabilities from 76% (565/743) in FY 2021 to 28% (286/1022) in FY 2022. Figure 1 below depicts AmeriCorps vulnerabilities by criticality and type.

Figure 1 also compares the vulnerability management program improvements from FY 2021 to FY 2022.[19]

[19] Other auditors performed independent network vulnerability scans in FY 2021.

Figure 1: AmeriCorps Critical and High Vulnerabilities Non-Credential Scan



Categories of Critical and High Vulnerabilities

We also focused on the Critical and High vulnerabilities, categorized them by their risk severity rating, and classified them into three general areas.

- **Misconfigurations**: Operating systems and applications that were poorly configured or contained default settings placed critical systems at unnecessary risk of unauthorized access, alteration, or destruction. Default settings are preconfigured settings placed in software to allow initial operation but are not set for security. These settings are the same for similar applications and are well-known on the Internet.

  We found 162 configuration weaknesses, including default passwords in applications and file access permissions, weak encryption, and Windows systems not configured for the least privilege (Figure 2).

- **Missing Patches**: Unpatched software contains known security flaws that exploitation techniques can easily be found on the Internet. AmeriCorps must apply the latest security patches from software vendors to mitigate known and unknown information security vulnerabilities.

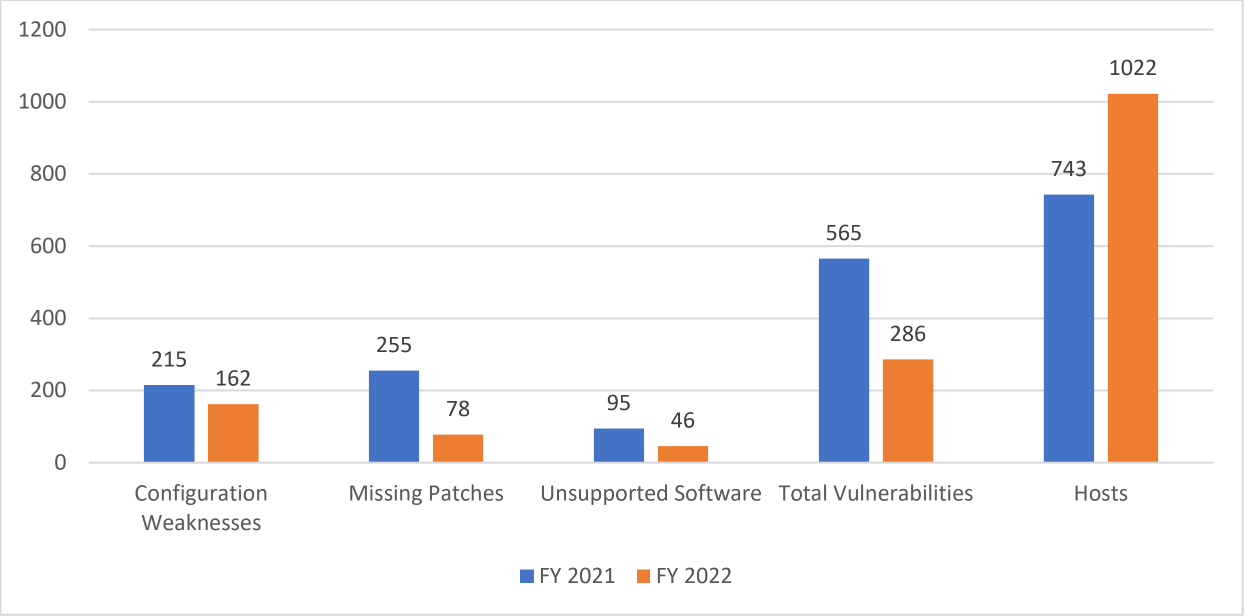
  We found 78 incidences where systems were missing patches, including VMware products, Microsoft products, system management software, and various other applications (Figure 2).

- **Unsupported Software**: Unsupported software is no longer supported by the vendors, and they do not offer security updates to remediate software flaws. Further, unsupported software may not be compatible and may not work with other systems or applications or limits systems or applications' use. The unsupported software can expose AmeriCorps to vulnerabilities that cannot be fully mitigated.

We found 46 incidences of unsupported software, including Microsoft SQL and Oracle databases, Windows operating systems, and Web Servers (Figure 2).

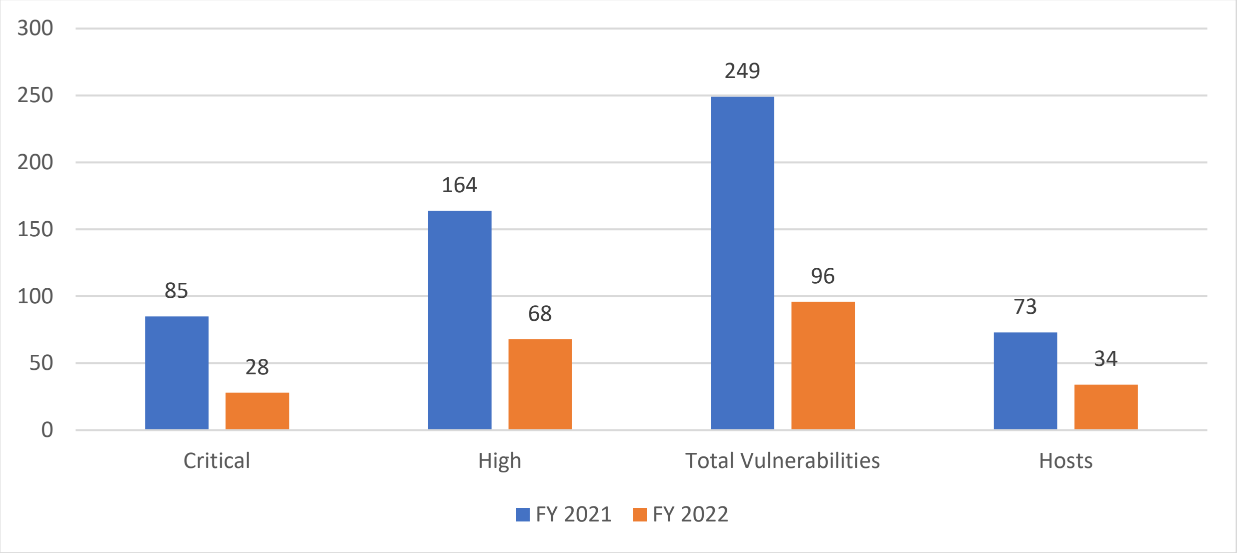
Figure 2 below shows that each category of weaknesses has decreased from the prior year.

Figure 2: AmeriCorps Critical and High Vulnerability Categories Non-Credential Scan



In FY 2021, the independent scan detected 73 Windows Operating systems; in FY 2022, we found only 34 Windows Systems. During FY 2022, AmeriCorps replaced the unsupported Windows operating system on its network to reduce the number of known vulnerabilities. By removing the older unsupported operating systems, AmeriCorps reduced the risk of security breaches or vulnerabilities discovered on those systems and helped improve the overall security of AmeriCorps. AmeriCorps' progress (Figure 3).

Figure 3: Vulnerabilities on Windows Workstations and Servers



We also found that AmeriCorps did not have an effective process for monitoring, detecting, and remediating known vulnerabilities. The longer the known vulnerability is exposed on the network, the greater the risk that the vulnerability can be exploited. Approximately 32 percent of the Critical and High vulnerabilities were over 13 months old. We found patches for Critical and High vulnerabilities were not applied timely, and vulnerabilities remained unmitigated, as depicted in Table 4 below. Critical vulnerabilities are required to be mitigated in seven days and 30 days for High vulnerabilities in accordance with AmeriCorps policies.

Table 4: Aging of Critical and High Vulnerabilities[20]

Vulnerabilities	Under 3 Months	3 to 6 Months	7 to 12 Months	13 to 24 Months	Over 24 Months	Total
Critical	7	10	82	12	2	113
High	40	48	9	27	49	173
Total	**47**	**58**	**91**	**39**	**51**	**286**
Percentage	**16%**	**20%**	**32%**	**14%**	**18%**	**100%**

[20] The Vulnerability rating of Critical and High vulnerabilities was based on a common and standardized vulnerability scoring system, Common Vulnerability Scoring System (CVSS) Version 3, to rate the severity of vulnerabilities shown below.

- Critical [CVSS score 10.0] – The attacker has direct access to the vulnerability with negligible access impediments or authentication barriers in place. Known exploits require minimal skill to perform. The end impact on confidentiality, integrity, and availability (CIA) is certain.
- High [CVSS score 7.0 – 9.9] – The attacker has direct access to the vulnerability on the target with minor access impediments or authentication barriers. Known exploits require little skill to perform. The end impact on the CIA is likely.

Known Exploited Vulnerabilities

DHS is authorized to develop and oversee the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidance developed by the Director of OMB and requirements of FISMA. DHS Binding Operational Directive is a compulsory direction to executive branch departments and agencies to safeguard federal information and information systems. On November 3, 2021, DHS issued the Binding Operational Directive 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities (KEV).

AmeriCorps was not in compliance with that Directive, which maintains the authoritative source of vulnerabilities exploited in-the-wild,[21] the Known Exploited Vulnerability catalog. These vulnerabilities carry significant risk to the Federal enterprise and establish requirements for agencies to remediate vulnerabilities listed in the catalog. Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the documented vulnerabilities to reduce the likelihood of compromise by known threat actors. We found 43 of 45 (96%) of KEVs are over three months old (Table 5). Table 5 also represents the analysis of outstanding KEV vulnerabilities requiring remediation within 14 days.

Table 5: Aging of KEV

Risk	Under 3 Months	3 to 6 Months	7 to 12 Months	13 to 24 Months	Over 24 Months	Total
KEV	**2**	**30**	**13**	**-**	**-**	**45**
Percentage	4%	67%	29%	-	-	100%

AmeriCorps policy states that the Information System Security Office (ISSO) is responsible for the following:

- Scanning for vulnerabilities in the information system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system/applications were identified and reported; and
- Remediating legitimate vulnerabilities in accordance with an organizational assessment of risk:
  - Critical – within seven days; and
  - High – within 30 days.

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

[21] In-the-wild is a term related to malicious software found on workstations belonging to ordinary users.

Management did not implement recommendations 1 and 2 from the FY 2019 FISMA evaluation report[22] to assist AmeriCorps in improving its vulnerability management program. These recommendations included implementing a process to track patching of network devices and servers by the defined risk-based patch timelines in AmeriCorps policy; replacing information system components when support is no longer available; monitoring and recording actions taken by the contractor to ensure vulnerability remediation for network devices and servers are addressed, or the exposure minimized and enhancing the inventory process to ensure all devices are properly identified and monitored. Therefore, these recommendations remain open. We are not issuing a new recommendation.

4. AmeriCorps Must Enforce Multifactor Authentication for Information System Users

FY 2022 IG FISMA Function: *Protect* / **Domain**: *Identity and Access Management*

Federal information systems must uniquely identify and authenticate users before granting access.[23] MFA requires users to authenticate with additional credentials other than solely a username and password. Examples include tokens or PIV credentials issued by Federal agencies. In addition, OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, issued May 21, 2019, states, "Agencies shall require PIV credentials (where applicable in accordance with [Office of Personnel Management] OPM requirements) as the primary means of identification and authentication to Federal information systems and Federally controlled facilities and secured areas by Federal employees and contractors."

AmeriCorps did not consistently implement strong authentication mechanisms (e.g., PIV cards) for all privileged and non-privileged users. Specifically, AmeriCorps did not enforce MFA for eight of 47 (17%) privileged users. Additionally, MFA was not enforced for 93 of 811 (11%) non-privileged users, 74 of 679 employees and 19 of 132 contractors, as depicted in Table 6.

Table 6: Multifactor Authentication

Users	No MFA	Population	Percentage
Total Privileged Users	**8**	**47**	**17%**
Non-privileged Users			
Employees	74	679	11%
Contractors	19	132	14%
Total Non-privileged Users	**93**	**811**	**11%**

AmeriCorps did not reinstate PIV enforcement in accordance with DHS CISA guidance. Most of the AmeriCorps workforce continued to telework during FY 2022 due to the COVID-19 pandemic. While AmeriCorps initiated an effort to ensure PIV compliance across the agency, the effort

[22] Recommendation 1 and 2, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, OIG Report Number 20-03 (January 24, 2020), Page 10.

[23] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, control IA-2, Identification and Authentication (Organizational Users), Page 132.

remains ongoing. Therefore, AmeriCorps will not be fully PIV-compliant until it limits access to its information systems (applications) via PIV or MFA only.

By not fully implementing MFA, AmeriCorps increases the risk of unauthorized access to its information systems and data, including Personally identifiable information (PII), which may result in personal harm, loss of public trust, legal liability, or increased costs of responding to a breach of PII. Identifications (ID)[24] and passwords are no longer an effective control. Further, AmeriCorps created increased risk by failing to enforce MFA for users with elevated access privileges, such as administrator rights and access to critical files and data.

Management did not implement recommendation 6 from the FY 2020 FISMA evaluation[25] and recommendations 8 and 9 from the FY 2021 FISMA evaluation report[26] to update AmeriCorps' policy to require and reinstate mandatory enforcement of MFA. Therefore, these recommendations remain open. We are not issuing a new recommendation.

5. AmeriCorps Must Utilize Qualitative and Quantitative Performance Metrics

FY 2022 IG FISMA Function: *Protect* / **Domain**: *Data Protection and Privacy*

Entity-wide performance metrics help decision-makers with the information, analysis, and recommendations they need to respond to this increasingly complex and interconnected environment. Entity-wide performance metrics are a part of an Enterprise Risk Management (ERM) program, that provides an objective analysis, for management and those charged with governance and oversight. Performance metrics can be used to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to the accountability of operations.

AmeriCorps did not use qualitative and quantitative performance metrics to measure, report, and monitor the information security performance of its:

- Data exfiltration and enhanced network defenses;
- Incidence detection and analysis process; and
- Incidence handling process.

NIST requires AmeriCorps to identify the specific analytic approach for the risk assessment, including the assessment approach (i.e., quantitative, qualitative, semi-quantitative) and the analysis approach (i.e., threat-oriented, asset/impact-oriented, vulnerability-oriented). [27] NIST also

[24] Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of ID.
[25] Recommendation 6, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, OIG Report Number EV-21-03 (December 18, 2020), Page 20.
[26] Recommendation 6, *Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, OIG Report Number EV-22-03 (December 15, 2021), Page 20.
[27] NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, Page 28.

requires *Performance Measurement*[28] that yields quantifiable information (percentages, averages, and numbers); data that supports the measures need to be readily obtainable; only repeatable information security processes should be considered for measurement, and measures must help track performance and direct resources.

Although AmeriCorps employed a process of performing risk assessments to determine the respective risk posture of its systems, the process was not enhanced to leverage and report in a broader array of quantitative and qualitative performance metrics. Without comprehensive entity-wide performance metrics, decision-makers may not be aware of the effectiveness of critical controls and activities, which may decrease AmeriCorps' ability to make risk-based decisions, improve performance, enhance accountability, and gauge success in accomplishing its mission.

We recommend:

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. (**New**)

[28] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, Pages 9 and 10.

Maturity Model Scoring

The maturity level based on the 8 IG FISMA Metrics for the "Protect" function is Level 2 (*Defined*), Not Effective, as depicted in Table 7.

Table 7: Security Function Protect Metrics

Maturity Level	Count	IG FISMA Metrics
Ad Hoc (Level 1)	-	N/A
Defined (Level 2)	3	21, 30 and 31
Consistently Implemented (Level 3)	2	36 and 37
Managed and Measurable (Level 4)	2	20 and 22
Optimized (Level 5)	1	42
Calculated Maturity Level: Defined (Level 2), Not Effective		

Security Function: Detect

6. AmeriCorps Must Conduct Annual Security Assessment for the Momentum System

FY 2022 IG FISMA Function: *Detect* / **Domain**: I*nformation Security Continuous Monitoring*

Security assessments and authorizations are comprehensive assessments that attest a system's security controls are meeting the security requirements and an official management decision to authorize the operation of an information system and accept its known risks. AmeriCorps did not consistently implement its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. Specifically, AmeriCorps did not perform an annual assessment as stated in its policies, including security and privacy controls and risk assessment for Momentum, one of the four systems selected for testing in accordance with its policies. Momentum's most recent security control and risk assessments were conducted in January 2021.

NIST requires AmeriCorps to perform control assessments and risk assessments. In addition, the AmeriCorps *Cybersecurity Control Families* document requires the Information System Security Officer (ISSO) and Security Assessment Team to assess the security controls in the information system and its environment of operation through continuous monitoring, and reviewing one-third of the controls annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome concerning meeting established security requirements.[29]

The AmeriCorps *Cybersecurity Control Families* document also requires the ISSO to update the system risk assessment annually or whenever significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

AmeriCorps' poor oversight resulted in missing the annual risk and security control assessment. Without consistently performing and documenting security control assessments and risk assessments for AmeriCorps systems, the authorizing official and other agency stakeholders may not be aware of security and privacy risks to the systems, potentially impacting the overall risk exposure to AmeriCorps. As a result, AmeriCorps may not be accurately measuring the risks of compromise of the confidentiality, integrity, and availability of AmeriCorps information and information systems.

We recommend:

2. AmeriCorps perform an annual security assessment and risk assessment for the Momentum application in accordance with AmeriCorps' policies. (**New**)

[29] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* CA-2 Pages 84 and 85 and RA-3 Pages 240 and 241.

Maturity Model Scoring

The maturity level based on the two IG FISMA Metrics for the "Detect" function is Level 2 (*Defined*) or Not Effective, as depicted in Table 8.

Table 8: Security Function Detect Metrics

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

The key control weaknesses affecting the "Detect" maturity level, including inconsistent mobile devices, asset management, vulnerability, configuration, MFA, security assessment and contingency planning management, affect the "Identify" and "Protect" functions and are addressed in those sections of this report.

Security Function: Respond
Maturity Model Scoring

The maturity level based on the two metrics IG FISMA Metrics for the "Respond" function area is Level 3 (*Consistently Implemented*) or Not Effective, as depicted in Table 9.

Table 9: Security Function Respond Metrics

Maturity Level	Count	IG FISMA Metrics
Ad Hoc (Level 1)	-	N/A
Defined (Level 2)	-	N/A
Consistently Implemented (Level 3)	3	54 and 55
Managed and Measurable (Level 4)	-	N/A
Optimized (Level 5)	-	N/A
Calculated Maturity Level: Consistently Implemented (Level 3), Not Effective		

Security Function: Recover

7. COOP Not Reviewed Annually

FY 2022 IG FISMA Function: *Recover* / **Domain**: *Contingency Planning*

COOP is a documented plan of activities needed by an agency to ensure it can continue to perform its essential functions during a wide range of events that affect normal operations. The COOP encompasses plans for the potential threat from equipment failure, human error, weather, natural disasters, and criminal or terrorist attacks.

AmeriCorps policies[30] and NIST standards[31] require an annual review. AmeriCorps did not update the COOP Plan as part of its annual review process. The previous plan was dated March 5, 2020. The plan was required to be reviewed by March 5, 2021. The plan review and revisions were overdue for 16 months until the new COOP was signed on July 14, 2022.

Without proper updates to the COOP plan, AmeriCorps may not be able to ensure that the agency can continue the performance of essential functions during a wide range of emergencies.

We recommend:

3. AmeriCorps implement the necessary oversight to monitor the COOP Plan review process to ensure the plan is updated annually. (**New**)

[30] Corporation for National and Community Service Continuity of Operations Plan, March 5, 2020, Page 5.

[31] NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems,* Page 9.

Maturity Model Scoring

The maturity level based on the two IG FISMA Metrics for the function area "Recover" is Level 4 (*Managed and Measurable)* or Effective, as depicted in Table 10.

Table 10: Security Function Recover Metrics

Maturity Level	Count	IG FISMA Metrics
Ad Hoc (Level 1)	-	N/A
Defined (Level 2)	-	N/A
Consistently Implemented (Level 3)	1	63
Managed and Measurable (Level 4)	1	64*
Optimized (Level 5)	-	N/A
Calculated Maturity Level: (Managed and Measurable Level 4), Effective		

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

Appendix I – Background

AmeriCorps[32] was established in 1993 to connect Americans of all ages and backgrounds with opportunities to give back to their communities and the nation. Its mission is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. AmeriCorps has a FISMA inventory of eight information systems – the Network or General Support System (GSS), eSPAN (which includes the eGrants grants management system), Momentum, AmeriCorps Health Benefits, AmeriCorps Childcare Benefits System, Presidential Volunteer Service Awards, Online Ordering system, and public websites. The first six of these systems are categorized as moderate security, while the Online Ordering system and public websites were rated as low security.[33] 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 high levels of service and reduce costs, AmeriCorps' Office of Information Technology (OIT) outsourced the operation, maintenance, and support of most of AmeriCorps' IT systems. Despite this, AmeriCorps, by law, retains responsibility for complying with the requirements of the FISMA and security control implementation. Consequently, AmeriCorps and its contractors share responsibility for managing the information systems.

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, which incorporates NIST SP 800-53, Revision 5.

FISMA Legislation

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires Federal agencies to develop, document, and implement an Agency-wide information security program to protect

[32] Effective on October 15, 2020, the operating name of the agency was changed from Corporation for National and Community Service to AmeriCorps.
[33] 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.

their information and information systems, including those provided or managed by another agency, contractor, or other sources.

The statute also provides a mechanism for improved oversight of Federal Agency information security programs. FISMA requires Agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the OMB and congressional committees on the effectiveness of their information security program.

Federal agencies are required to provide information security protections commensurable to the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the Agency. As specified in FISMA, the Agency CIO or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires the Agency's IG to assess the effectiveness of agency information security programs and practices. Guidance was issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the Federal Information Processing Standards to establish Agency baseline security requirements.

FY 2022 IG FISMA Reporting Metrics

On December 6, 2021, OMB and DHS provided instructions to Federal agencies and IGs for preparing FISMA reports annually. OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements.* This memorandum describes the processes for federal agencies to report to OMB and, where applicable, DHS. Accordingly, the F Y22 Core IG Metrics Implementation Analysis and Guidelines (Core IG FISMA Metrics) provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[34]

The FY 2022 IG FISMA Metrics incorporate a maturity model that aligns with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1 Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise IT and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in Table 11.

[34] FY22 Core IG Metrics Implementation Analysis and Guidelines (cisa.gov).

Table 11: Aligning NIST Cybersecurity Framework Security Functions to the FY 2022 IG FISMA Metric Domains

NIST Cybersecurity Framework Security Functions	FY 2022 IG FISMA Metrics Domains
Identify	Risk Management and Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

A functional information security area is not considered effective unless it achieves a rating of at least Level 4 (*Managed and Measurable*). Table 12 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 12: IG Evaluation Maturity Levels

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

Appendix II – Objective, Scope, and Methodology

Objective

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

Scope

We conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation,* issued by the Council of Inspectors General on Integrity and Efficiency.[35] The evaluation was designed to assess the effectiveness of AmeriCorps' information security program in accordance with FISMA, OMB requirements, and NIST guidance.

The overall scope of the FISMA evaluation was the review of relevant security programs and practices to report on the effectiveness of AmeriCorps' Agency-wide information security program in accordance with the OMB's annual FISMA reporting instructions. We reviewed controls specific to FISMA reporting, including the process and practices AmeriCorps implemented for safeguarding PII and reporting incidents involving PII, protecting sensitive information, and management oversight of contractor-managed systems.

The evaluation included the testing of select management, technical, and operational controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, for the following information systems:

- GSS;
- eSPAN;
- My AmeriCorps Portal (a subsystem of eSPAN); and
- Momentum.

The evaluation was conducted remotely due to the restrictions caused by the COVID-19 pandemic from June 13, 2022, to November 15, 2022. A network vulnerability assessment was also conducted at HQ.

In addition, the evaluation included an assessment of effectiveness for each of the nine[36] FY 2022 IG FISMA Metrics Domains and the maturity level of the five Cybersecurity Framework Security Functions. The evaluation also included a follow up on prior years' recommendations to determine whether AmeriCorps made progress in implementing the recommended improvements concerning its information security program.[47]

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

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 2022 IG FISMA Metrics Domains aligned with the Cybersecurity Framework Security Functions. Table 13 lists the selected controls for the four AmeriCorps systems reviewed for this evaluation.

Table 13: List of Selected Controls Reviewed

Security Control Family	NIST 800-53 Associated Control
Access Control	AC-1, AC-2, AC-5, AC-6, and AC-17
Audit And Accountability	AU-2, AU-3, and AU-6
Awareness And Training	AT-2, and AT-3
Security Assessment and Authorization	CA-2, CA-3, CA-5, CA-6, and CA-7
Configuration Management	CM-3, CM-6, CM-7, CM-8, CM-10, and CM-11
Contingency Planning	CP-2, CP-3, and CP-4,
Identification And Authentication	IA-2, IA-4, IA-5, and IA-8
Incident Response	IR-4, IR-5, and IR-6
Media Protection	MP-3 and MP-6
Physical And Environmental Protection	PE-3
Planning	PL-2
Program Management	PM-5, PM-6, PM-9, PM-10, PM-13, PM-14, and PM-31
Risk Assessment	RA-3, RA-5, and RA-9
Supply Chain Risk Management	SR-3, SR-5, and SR-6
System And Services Acquisition	SA-4
System And Information Integrity	SI-2, SI-3, SI-4, and SI-7
System And Communications Protection	SC-7, SC-8, and SC-18

To accomplish the evaluation objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to AmeriCorps' information security program, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan, and continuous monitoring plan.
- Tested system processes to determine the adequacy and effectiveness of selected controls. Reviewed the status of recommendations in the FY 2021 FISMA report, including supporting

documentation, to ascertain whether the actions taken addressed the weakness.[37] See Appendix III for the status of prior years' recommendations.

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

- Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.
- FY 2022 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 review). In some cases, this resulted in selecting the entire population. However, in cases where the entire evaluation population was not selected, the results cannot be projected and, if projected, may be misleading.

[37] *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).

Appendix III – Status of Prior Year Recommendations

During FY 2022, AmeriCorps implemented corrective actions to close 12 prior years' recommendations from the FY 2017 to FY 2021 FISMA evaluations. The remaining 30 recommendations are open, as depicted in Table 14, and there are three new FY 2022 recommendations, as mentioned in this report.

Table 14: Status of Prior Years' Recommendations

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
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	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 26: Ensure the facilities implement the following in regard to protection of mobile devices: • Enforce the prohibition of displaying passwords in public view. • Require the use of passwords on mobile computer assets for all users. • Change passwords and re-image IT assets upon the separation of the previous user. • Monitor Team Lead laptops for compliance with security updates and antivirus signatures. • Prohibit the use of non-governmental AmeriCorps issued email accounts. • Configure cell phones to require the enabling of security functions	Open	Open AmeriCorps stated they were in progress in closing the recommendation.

[38] Status as of June 9, 2022.

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
Recommendation 27: Ensure the facilities implement the following in regard to protection of mobile devices: • Require the use of passwords on mobile computer assets for all users. • Change passwords and re-image IT assets upon the separation of the previous user. • Prohibit the use of non-governmental AmeriCorps issued email accounts.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
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 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 are addressed or the exposure to unpatchable vulnerabilities is minimized. • Enhance the inventory process to ensure all devices are properly identified and monitored.	Open	Open AmeriCorps stated they were in progress in closing the recommendation. RMA confirmed the recommendation was still open. Refer to Finding 3

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
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	Open AmeriCorps stated they were in progress in closing the recommendation.
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	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 5: Develop and implement a written process to ensure RemedyForce tickets are completed at the time the inventory is updated.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 6: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 7: Perform and document analysis to determine the feasibility of completely automating the inventory management process.	Open	Open AmeriCorps stated they were in progress in closing the recommendation. RMA confirmed the recommendation was still open. Refer to Finding 2
Recommendation 8: Continue the current effort to complete a comprehensive risk register at the mission and business process level.	Closed	Closed

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
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.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 10: Establish and document standard baseline configurations for all platforms in the AmeriCorps information technology environment and ensure these standard baseline configurations are appropriately implemented, tested, and monitored for compliance with established AmeriCorps security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Closed	Closed
Recommendation 11: Implement Personal Identification Verification multifactor authentication for local and network access for privileged users to all workstations and servers.	Open	Open AmeriCorps stated they were in progress in closing the recommendation. RMA confirmed the recommendation was still open. Refer to Finding 4

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
Recommendation 12: Complete the implementation of Personal Identification Verification multifactor authentication for network access for all non-privileged users by upgrading all users to Microsoft Windows 10 workstations and enforcing logon with a Personal Identification Verification card.	Open	Open AmeriCorps stated they were in progress in closing the recommendation. RMA confirmed the recommendation was still open. Refer to Finding 4
Recommendation 14: Enhance information systems to automatically disable user accounts after 30 days of inactivity in accordance with AmeriCorps policy. This includes monitoring automated scripts to validate accounts are disabled properly.	Closed	Closed
Recommendation 16: Develop and Implement a written process that ensures all AmeriCorps information system passwords are changed at the frequency specified in applicable AmeriCorps policy or the System Security Plan.	Closed	Closed
Recommendation 23: Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
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	Open AmeriCorps stated they were in progress in closing the recommendation.

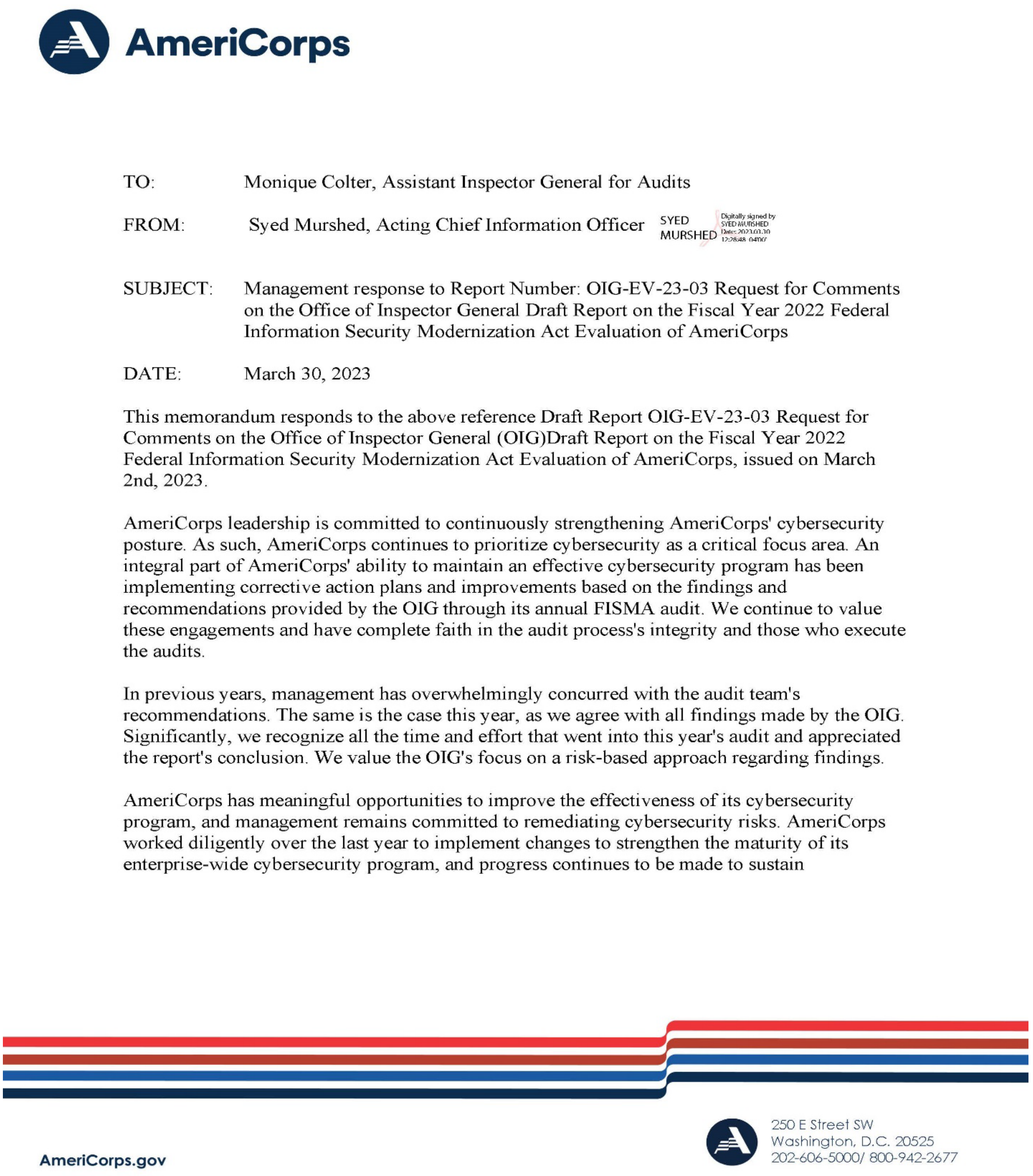
Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
Recommendation 29: Perform an analysis of the IG FISMA Metrics related to the security function "Protect" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board, which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program.	Closed	Open AmeriCorps provided no evidence to support closure.
Recommendation 30: Develop and implement a written process to review and analyze the wireless network logs at the NCCC Pacific and Southwest Regional Campuses.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
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	Open AmeriCorps provided no evidence to support closure.
FY 2020		
Recommendation 1: Perform and document an oversight process to ensure physical inventory reviews and updates are fully documented to include the exact location of all information technology assets	Closed	Closed This recommendation was superseded by FY 2021 Recommendation 2.
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.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
Recommendation 3: Develop and implement a process to block unauthorized applications from installing on CNCS mobile devices.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 4: Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations.	Open, Waiting for Departmental Closeout	Open AmeriCorps provided no evidence to support closure.
Recommendation 5: Fully implement standard baseline configurations for all platforms in the CNCS information technology environment and establish processes to test and monitor for compliance with established CNCS security standards.	Open, Waiting for Departmental Closeout	Closed RMA testing showed the recommendation was implemented.
Recommendation 6: Assess and document a plan for reinstating mandatory enforcement of multifactor authentication as recommended by the Cybersecurity and Infrastructure Security Agency to address increased risks with the large number of personnel teleworking during the pandemic.	Open	Open AmeriCorps stated they were in progress in closing the recommendation. RMA confirmed the recommendation was still open. Refer to Finding 4
Recommendation 8: Ensure that accounts for users that never logged in are included in the CNCS Inactive script.	Closed	Closed
Recommendation 9: Ensure all personnel whose responsibilities include access to PII complete annual privacy-role based training.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
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	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 2: Complete asset tracking refresher training for the Tier 2 support team.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
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.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 4: Complete and execute the ISA with the Social Security Administration.	Open	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.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
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	Open AmeriCorps stated they were in progress in closing the recommendation.

Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations[38]
Recommendation 7: Update the SIA SOP to require maintaining completed SIA questionnaires in the change management tool for all system changes for validating whether each configuration change requires an SIA.	Closed	Closed
Recommendation 8: Immediately reinstate mandatory enforcement of multifactor authentication in accordance with CISA's recommendation.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 9: Update AmeriCorps' policy to require mandatory enforcement of multifactor authentication in the future, including in any hybrid work environment.	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
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	Open	Open AmeriCorps stated they were in progress in closing the recommendation.
Recommendation 11: Design and implement a method for identifying inactive privileged accounts via an automated script and manually disabling those accounts, as needed.	Open	Closed RMA testing showed the recommendation was implemented.
Recommendation 12: Perform an annual incident response test or exercise in accordance with AmeriCorps' policies.	Closed	Closed
Recommendation 13: Establish an oversight process to ensure that the MITS Disaster Recovery Plan is tested for the GSS and eSPAN and associated training is conducted on an annual basis.	Closed	Closed

Appendix IV – Management Comments



AmeriCorps

TO: Monique Colter, Assistant Inspector General for Audits

FROM: Syed Murshed, Acting Chief Information Officer SYED MURSHED Digitally signed by SYED MURSHED Date: 2023.03.30 12:28:48 -04'00'

SUBJECT: Management response to Report Number: OIG-EV-23-03 Request for Comments on the Office of Inspector General Draft Report on the Fiscal Year 2022 Federal Information Security Modernization Act Evaluation of AmeriCorps

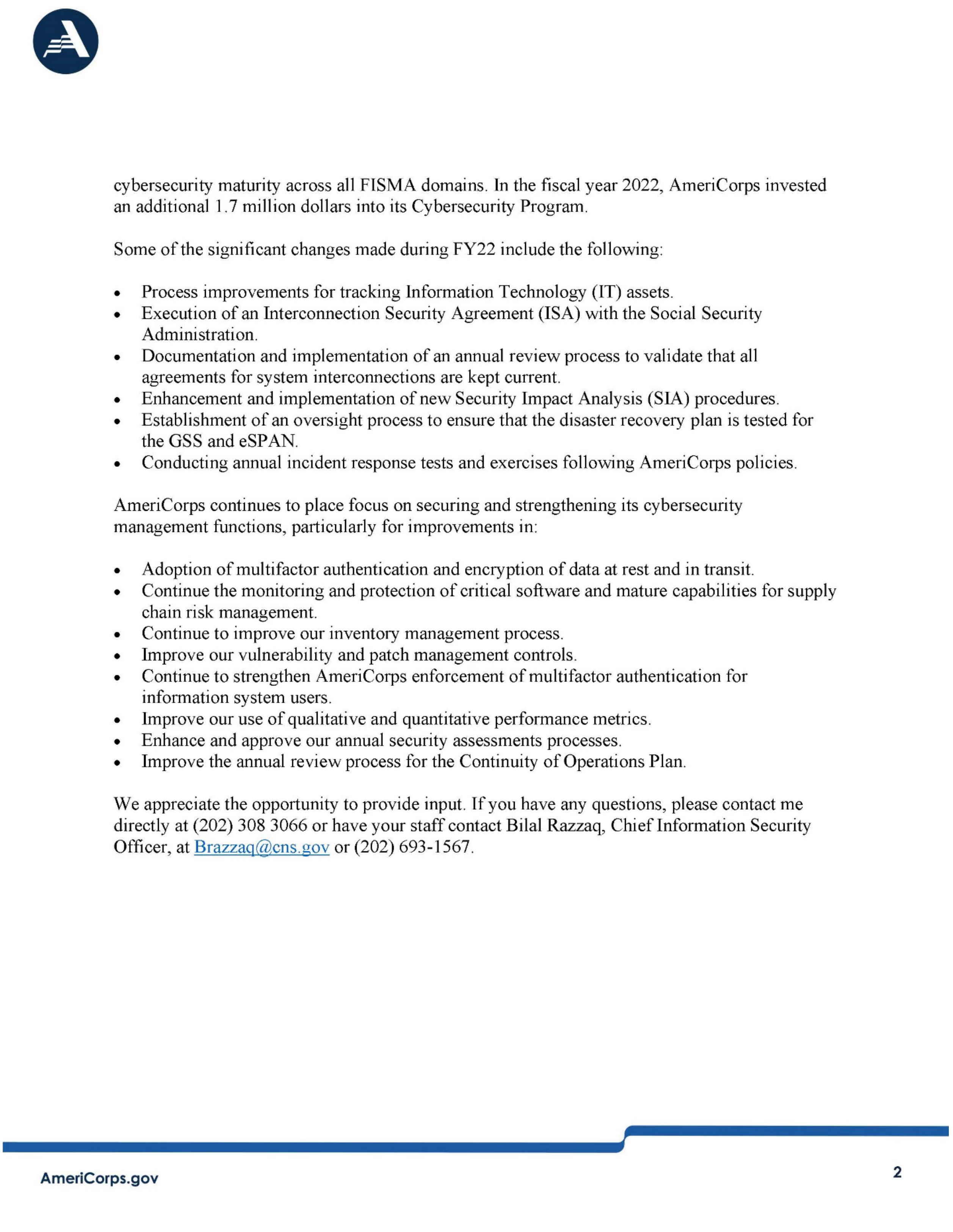
DATE: March 30, 2023

This memorandum responds to the above reference Draft Report OIG-EV-23-03 Request for Comments on the Office of Inspector General (OIG)Draft Report on the Fiscal Year 2022 Federal Information Security Modernization Act Evaluation of AmeriCorps, issued on March 2nd, 2023.

AmeriCorps leadership is committed to continuously strengthening AmeriCorps' cybersecurity posture. As such, AmeriCorps continues to prioritize cybersecurity as a critical focus area. An integral part of AmeriCorps' ability to maintain an effective cybersecurity program has been implementing corrective action plans and improvements based on the findings and recommendations provided by the OIG through its annual FISMA audit. We continue to value these engagements and have complete faith in the audit process's integrity and those who execute the audits.

In previous years, management has overwhelmingly concurred with the audit team's recommendations. The same is the case this year, as we agree with all findings made by the OIG. Significantly, we recognize all the time and effort that went into this year's audit and appreciated the report's conclusion. We value the OIG's focus on a risk-based approach regarding findings.

AmeriCorps has meaningful opportunities to improve the effectiveness of its cybersecurity program, and management remains committed to remediating cybersecurity risks. AmeriCorps worked diligently over the last year to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program, and progress continues to be made to sustain



cybersecurity maturity across all FISMA domains. In the fiscal year 2022, AmeriCorps invested an additional 1.7 million dollars into its Cybersecurity Program.

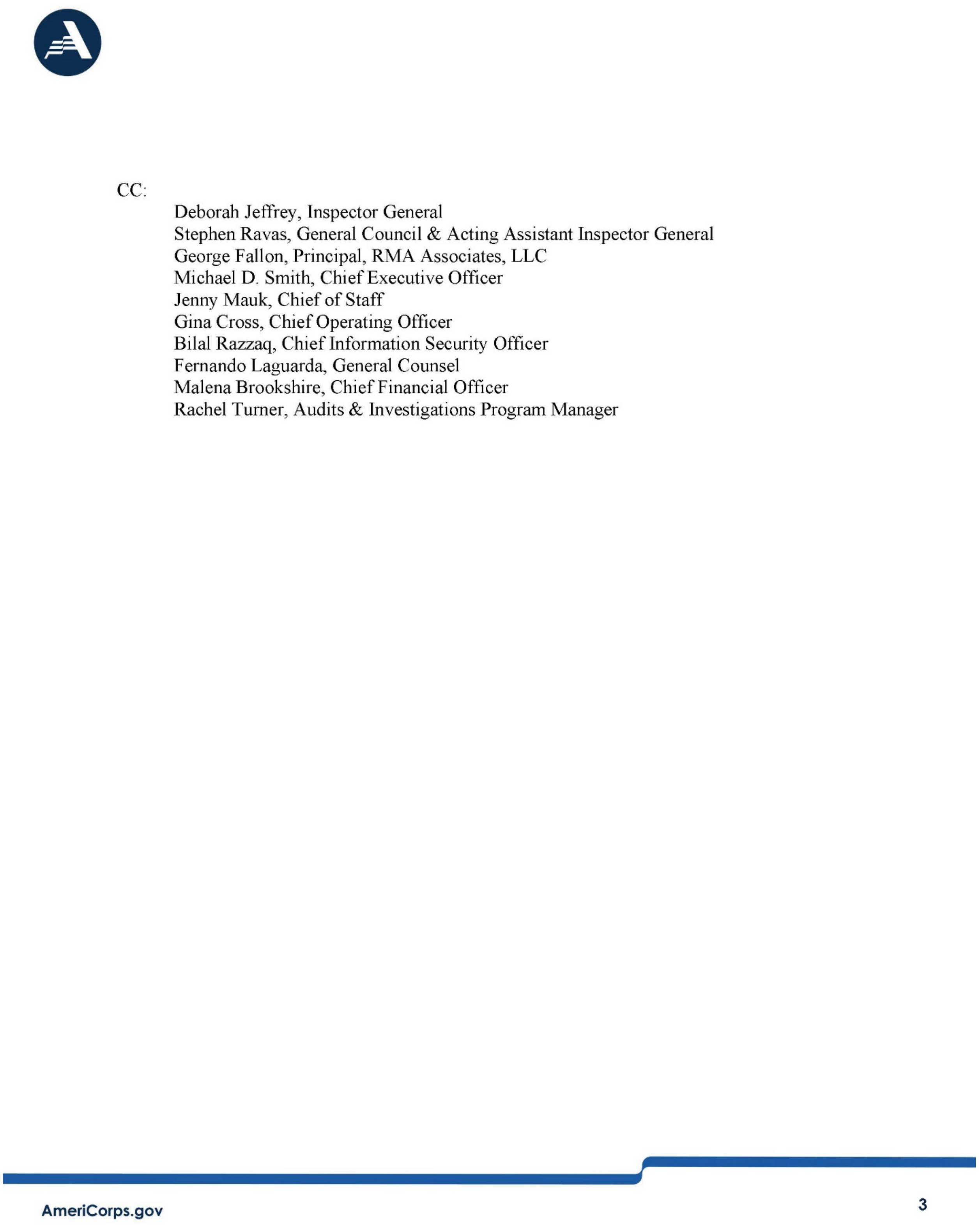
Some of the significant changes made during FY22 include the following:

- Process improvements for tracking Information Technology (IT) assets.
- Execution of an Interconnection Security Agreement (ISA) with the Social Security Administration.
- Documentation and implementation of an annual review process to validate that all agreements for system interconnections are kept current.
- Enhancement and implementation of new Security Impact Analysis (SIA) procedures.
- Establishment of an oversight process to ensure that the disaster recovery plan is tested for the GSS and eSPAN.
- Conducting annual incident response tests and exercises following AmeriCorps policies.

AmeriCorps continues to place focus on securing and strengthening its cybersecurity management functions, particularly for improvements in:

- Adoption of multifactor authentication and encryption of data at rest and in transit.
- Continue the monitoring and protection of critical software and mature capabilities for supply chain risk management.
- Continue to improve our inventory management process.
- Improve our vulnerability and patch management controls.
- Continue to strengthen AmeriCorps enforcement of multifactor authentication for information system users.
- Improve our use of qualitative and quantitative performance metrics.
- Enhance and approve our annual security assessments processes.
- Improve the annual review process for the Continuity of Operations Plan.

We appreciate the opportunity to provide input. If you have any questions, please contact me directly at (202) 308 3066 or have your staff contact Bilal Razzaq, Chief Information Security Officer, at Brazzaq@cns.gov or (202) 693-1567.



CC:

Deborah Jeffrey, Inspector General
Stephen Ravas, General Council & Acting Assistant Inspector General
George Fallon, Principal, RMA Associates, LLC
Michael D. Smith, Chief Executive Officer
Jenny Mauk, Chief of Staff
Gina Cross, Chief Operating Officer
Bilal Razzaq, Chief Information Security Officer
Fernando Laguarda, General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits & Investigations Program Manager

Appendix V – Evaluation of Management Comments

Based on our evaluation of management comments, we acknowledge AmeriCorps' management decisions on the new three recommendations and believe the actions taken and planned will resolve the issues identified in the report.

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