



AmeriCorps

OFFICE OF INSPECTOR GENERAL

AMERICORPS PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION

FINAL AUDIT REPORT

NUMBER: OIG-EV-22-06

July 21, 2022

OFFICE OF INSPECTOR GENERAL



OFFICE OF INSPECTOR GENERAL
AmeriCorps

July 21, 2022

MEMORANDUM TO: Syed Murshed
Acting Chief Information Officer

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

SUBJECT: Office of Inspector General Final Evaluation Report, OIG-EV-22-06:
AmeriCorps' Penetration Testing and Phishing Campaign

Enclosed is the Office of Inspector General's Final Evaluation Report, OIG-EV-22-06: *AmeriCorps' Penetration Testing and Phishing Campaign*. The evaluation was conducted by CliftonLarsonAllen LLP (CLA) in accordance with *Quality Standards for Inspections and Evaluations* issued by the Council of Inspectors General on Integrity and Efficiency. If you have any questions or wish to discuss the draft report, please contact me at (202) 875-0245 or m.colter@americorpsoig.gov.

cc: 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
Jill Graham, Chief Risk Officer
Rachel Turner, Audits, and Investigations Program Manager
Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

**AmeriCorps
Penetration Testing and Phishing Campaign Evaluation**

July 20, 2022

Final Report



CPAs | CONSULTANTS | WEALTH ADVISORS

[CLAconnect.com](https://www.CLAconnect.com)

TABLE OF CONTENTS

Introduction.....	1
Results in Brief.....	1
Evaluation Results	2
Appendix I – Objective, Scope, and Methodology.....	6
Appendix II – Management Comments	11

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

INTRODUCTION

AmeriCorps' security program has not been effective in accordance with Federal Information Security Management Act (FISMA), Office of Management and Budget requirements, and guidance from the National Institute of Standards and Technology since FY 2017.¹ The AmeriCorps Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA), an independent certified public accounting firm, to conduct an internal penetration test of AmeriCorps' network to provide additional areas of improvement towards having an effective information security program.

CLA conducted testing of AmeriCorps' network, the General Support System (GSS) that supports the AmeriCorps' Headquarters (HQ) and also a phishing campaign targeting a subset of all AmeriCorps' email users. CLA's evaluation was based on the approved Rules of Engagement (ROE) between AmeriCorps, the OIG, and CLA. CLA performed testing from February 14, 2022, through March 11, 2022, which provided a snapshot in time of the security control effectiveness during the testing period.

The evaluation was comprised of three phases. This first phase consisted of a network penetration test of the GSS at HQ. The second phase consisted of a phishing campaign whereby phishing emails were sent to a randomly selected sample from all AmeriCorps email users. The third phase was testing the effectiveness of the controls in preventing and detecting the execution of malicious code on AmeriCorps laptops. AmeriCorps provided CLA with a typical laptop that an AmeriCorps user would use in a remote employee scenario. The testing of the execution of malicious code was performed on this laptop.

RESULTS IN BRIEF

Our testing found two weaknesses of the AmeriCorps' information security program related to preventive and detective security controls.

- We discovered an exploitable vulnerability that could result in a complete system compromise. The vulnerability could allow unauthorized access to the target system, and

¹ *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 18-03, December 18, 2017).

Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service (OIG Report No. 19-03, March 1, 2019).

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).

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

Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of AmeriCorps, (OIG Report No. 22-03, December 15, 2021).

AMERICORPS PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION

there were no effective controls in place to identify malicious activities once on the system. If an exploitable system were compromised, the malicious attacker could operate for an extended time without detection.

- A second weakness was the number of users who succumbed to a phishing attempt by interacting with the content of a spam email. Systemically, AmeriCorps' controls for automated detection of phishing were not effective in prohibiting the email from arriving in the user's inbox. In addition, nine out of 85 users interacted with one of four different phishing emails. Had the attack been malicious, AmeriCorps' systems and data would have been compromised. Stronger behavioral training can make staff more resistant to phishing emails and less likely to interact with potentially malicious content. The current situation, in which potentially malicious spam emails can reach inadequately trained users increases the potential of successful attacks, resulting in a system compromise impacting confidentiality, integrity, and availability of the technology environment.

EVALUATION RESULTS

Except for the weaknesses noted below, the security controls tested were operating effectively. The controls regarding unwanted emails and malicious activity detection could be improved. The following sections provide details of each area of testing, along with three recommendations to help AmeriCorps improve its information security environment.

Network Penetration Testing

The purpose of the penetration testing was to identify and exploit vulnerabilities and insufficiently configured security controls to determine whether a user could obtain unauthorized access or elevated privileges to AmeriCorps' IT operational environment.²

Initially, we performed a unauthenticated Nessus vulnerability scan.³ The results provided a listing of 746 vulnerabilities with known exploits, which represented six unique vulnerabilities with known exploits appearing on multiple hosts. All but one of these exploits required an authenticated user to interact with a link to another computer that would deliver a malicious code to take advantage of the vulnerability. The one vulnerability we chose to exploit was selected because it did not require interaction with any logged-on users. This one vulnerability was in a software program installed on a system that had a publicly available exploit. The patch to fix this vulnerability was recently distributed by the vendor. However, the patch was not available in the latest monthly AmeriCorps patch cycle and therefore the system was still

² See Scope in Appendix I for additional information.

³ Nessus is a vulnerability scanner developed by Tenable, Inc. Nessus works by testing the operating system and each network service and program for missing patches, weak authentications, and configuration weaknesses. Nessus can be configured to authenticate to the system and report vulnerabilities from the perspective of an authenticated user. Nessus can also be used with no operating system authentication to report vulnerabilities from a non-authenticated network perspective. Each type of scan uses different vulnerability tests called plugins to search for different vulnerabilities.

AMERICORPS PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION

vulnerable. Once notified of the missing patch, the AmeriCorps Office of Information Technology (OIT) was able to apply the patch and remediate the risk.

In addition, we were able to execute the exploit and gain unauthorized, privileged access to the system. By gaining privileged access, we extracted the password file⁴ and attempted to crack the hashed format of the stored passwords. However, the password cracking was unsuccessful, demonstrating that administrative passwords being used incorporate an adequately complex scheme. We also inspected the system for connections to other hosts which would expand our unauthorized access to other hosts. We were not able to access other hosts.

Execution of Malicious Code

We tested the effectiveness of AmeriCorps' preventive and detective security controls over malicious code. We generated several types of malicious files to test controls on a typical AmeriCorps user workstation. Certain types of files were identified containing potentially harmful components and were blocked from execution by local host preventive controls. Other types of files were allowed to execute; however, the malicious functions were not allowed to complete to a level of exploitation. In this case, AmeriCorps' preventive controls recognized the abnormal, malicious intent of the file and prohibited the complete execution. In each case, the control generated a warning visible to the user alerting them of the exploit attempt.

Phishing Campaign

Finally, our phishing campaign delivered phishing emails to 85 user mailboxes⁵; nine of those users clicked a link to a server in the CLA Secure Network. Four of those nine users opened the link in a set of phishing emails that requested the recipient to click a link to review documents. The email narrative contained a sense of urgency and seemed to come from an authoritative source. Two of the nine users opened a phishing email that contained a message which appeared to inform the recipient of an undelivered email and requested the user to follow a link in the email to resend the message in question. Three of the nine users opened the link in the last set of phishing emails that notified the recipient of pending spam and requested the user to click a link to either identify the message in question as spam or allow the email to be delivered. Management communicated that phishing campaigns are conducted quarterly, and security awareness training is done annually. Subsequent training is provided to users who fail internal phishing tests.

⁴ In Linux systems, the local user accounts and passwords are stored in files `/etc/passwd` and `/etc/shadow` as a standard configuration. The actual password is stored as an encrypted string. There are several publicly available programs designed to reverse engineer (crack) these passwords depending on the password length and complexity.

⁵ During the phishing campaign we sent nine unique phishing emails and distributed those nine emails to 85 unique users. Each of the 85 users received one of these unique nine phishing emails.

AMERICORPS PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION

CONCLUSION

In most instances the existing controls performed in an effective manner in support of a safe and secure technology environment. However, the penetration test identified a workable exploit during the testing period that could be leveraged into a ransomware attack or lead to other systems being compromised. Exploitable vulnerabilities occur on a continuous basis; what appears safe and secure one day can be compromised the next day.

The phishing campaign exposed weaknesses in the following areas:

- The message was delivered into the user inbox; however, there was no indication to the recipient that the email originated from an external source.
- There were indicators in each of the phishing emails, mainly the source of the email. Preventive controls could have assisted the recipient to indicators that questioned the authenticity of these emails.

Phishing attacks are a constant threat and are becoming increasingly sophisticated. Users are responsible for protecting data and complying with information security directives, laws, and regulations. Phishing emails can result in financial damage from ransomware attacks, loss of productivity due to recovery of compromised computer systems, and impact the confidentiality, integrity, and authenticity of the entire data network.

RECOMMENDATIONS

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

Recommendation 1: Develop and implement a plan to modify external emails to include information to assist the recipient of the level of risk posed by external email. For example, the Subject line of an email should be modified to identify the source of the email as external to the agency. In addition, the body of the email should contain warnings concerning the dangers of external email and attachments. Finally, warnings should include how frequently the sender has interacted with the recipient.

Recommendation 2: Implement a plan to increase the frequency of behavior training directed at the identification of unwanted spam emails with an emphasis on continual reminders of recognition techniques, appropriate actions, and confidence that self-reporting poor behavioral actions will lead to a better outcome in the future.

Recommendation 3: Implement a process to improve the detection rate to reduce the occurrence of email spam that reaches the users' inboxes.

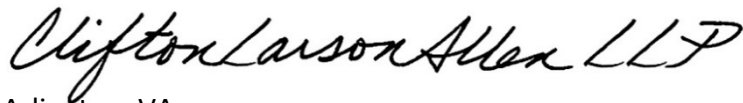
**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Management's Response and Evaluator's Comments

In response to the draft report, AmeriCorps concurred with all three recommendations, and provided corrective actions and a target date of implementation for each recommendation. We concur with management's planned actions. AmeriCorps' comments are included in their entirety in [Appendix II](#).

[Appendix I](#) describes the evaluation objective, scope, and methodology.

CliftonLarsonAllen LLP

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style.

Arlington, VA

July 20, 2022

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Appendix I

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this internal penetration test and phishing campaign was to assess security configurations and security control effectiveness by performing coordinated network-based and host-based security testing. Testing was designed to accomplish a better awareness of existing operational effectiveness. Specifically:

- To assess the technical security controls by performing coordinated network security tests;
- To determine the effectiveness of the security program in preventing and detecting unauthorized internal access to logical assets;
- Use compromised resource(s) and device(s) as a pivot point for future attacks; and
- To conclude on the effectiveness of the security administration and logical access controls.

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.⁶ The scope of the internal penetration test and phishing campaign was AmeriCorps' network, GSS for which AmeriCorps has security oversight that covers the AmeriCorps' HQ. Specific Internet Protocol address ranges and targets were outlined in the ROE.

We performed our testing from February 14, 2022, through March 11, 2022. This provided a snapshot in time of the security control effectiveness during the testing period.

The purpose of penetration testing was to identify and exploit vulnerabilities and insufficiently configured security controls to determine whether a user could obtain unauthorized access or elevated privileges to AmeriCorps' IT operational environment. Specifically, this testing examined whether technical weaknesses were present in the AmeriCorps' computer systems that may allow employees, contractors, or outsiders to inflict harm to, attack, and/or impact AmeriCorps' processes and information. In the context of this assessment, an outsider was defined as an individual or organization external to the agency that poses a threat to information security. Trusted insiders have an advantage over others who may want to harm an organization because an insider is a member of the organization with defined access such as a system

⁶ <https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf>

AMERICORPS

PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION

Appendix I

administrator, database administrator or end user who has knowledge of their organization's vulnerabilities, such as loosely enforced policies and procedures, or exploitable technical flaws. Even insiders who do not intend to cause harm may inadvertently do so through human error.

An additional approach to security testing is using the trusted insider perspective to discover the effectiveness of security controls as they pertain to everyday processes. In this phase, we tested the ability to elevate privileges and identify the probability that an existing security weakness could be exploited. If any existing configurations were exploited, we determined to what limit that exploitation could be discovered, monitored, and investigated. Our approach was to test AmeriCorps' ability to identify, contain and recover from any exploitable weakness we found within the network environment. In order to demonstrate this perspective, AmeriCorps allowed entry into the network and allowed the tests to be performed under the trusted user scenario. CLA worked with the AmeriCorps' technicians to understand if exploit attempts were identified as such and if the subsequent actions were traceable and reportable for forensic investigations.

Methodology

Internal Penetration Testing

The internal penetration testing was performed from inside a firewall using a CLA testing laptop placed on the internal GSS network and remotely accessible by CLA technicians. In addition, AmeriCorps provided CLA testing personnel with a typical laptop that an AmeriCorps user would use in a remote employee scenario on which CLA performed exploitations to minimize any network disruptions caused by exploitation testing. The internal testing consisted of four phases:

- Discovery
- Vulnerability Analysis
- Exploitation
- Reporting

A. Discovery

During the discovery phase, CLA attempted to obtain information about the AmeriCorps network, its operations, and practices, in addition to the activities and habits of its employees. To obtain this information, CLA used public sources and network identification utilities for internal testing.

B. Vulnerability Analysis

The purpose of this analysis or verification was to validate any potential vulnerabilities found during the discovery phase. CLA conducted verification in collaboration with the AmeriCorps technical team.

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Appendix I

Comparing the results of CLA's network security tests with AmeriCorps' policies and procedures highlighted areas in which current practices were not consistent with approved policies and procedures. In addition, comparing AmeriCorps' policies, procedures, and the results of CLA's network security tests with Federal standards and guidance spotlighted areas in which AmeriCorps can improve its security posture. These tests, coupled with an understanding of AmeriCorps' security policies and assessment and authorization process, provided a basis to conclude on the effectiveness of the AmeriCorps security administration and logical access controls.

C. Exploitation

Based on results of the vulnerability analysis, CLA used commercially available tools and customized scripts to conduct the internal network security tests. CLA conducted internal penetration testing attacks to identify methods for circumventing the security features of AmeriCorps application, systems or networks based on a target list of vulnerabilities for exploitation. To improve the value of CLA's tests, CLA used an overt or "white box" testing methodology. Further, CLA coordinated with AmeriCorps on testing techniques, progress, and success or failure. Using the feedback from AmeriCorps personnel, CLA adjusted and refined exploitation techniques to determine any threshold of effectiveness of preventive and detective controls in place. CLA targeted exploitation of AmeriCorps' system(s) generally required some knowledge of the system(s) and any inside attacker would be in possession of such information. AmeriCorps' credentials provided to CLA for credentialed scanning were not used in internal penetration testing attacks.

Exploitation was limited to demonstrating that a specific vulnerability existed and could be used to compromise network security on a sample of identified vulnerable hosts, of which CLA attempted to exploit known vulnerabilities.

It was understood and agreed that system states on the network devices under test would not undergo modification during the testing of vulnerabilities for exploit by CLA. This requirement was in place until CLA completed its testing.

D. Reporting

During the reporting phase we made actionable recommendations that can be used to move AmeriCorps' vulnerability management program forward and help them improve the overall effectiveness of their program. CLA provided the raw vulnerability data files to both OIG and AmeriCorps' management during the reporting phase after completion of testing.

AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION

Appendix I

Phishing Campaign

CLA conducted a phishing campaign with two key performance indicators of the effectiveness of security awareness training and technical controls designed to detect and prohibit system compromise. The endpoint computer was a valued target by being a trusted system on the network operated by a trusted user with degrees of access into critical technical assets. We designed a scenario through an email message to entice the target user to interact with the email message and that also tested the effectiveness of the security awareness training program within AmeriCorps. This was the first phase of the phishing campaign, getting interaction with the user.

Upon any interaction, the email message could initiate malicious activity which results in a system compromise. While this is the real-world progression of a phishing attack, CLA used a strategic alternative to deployment of malicious code and exploitation throughout the AmeriCorps environment. CLA used a dedicated, standard AmeriCorps computer as a dedicated target to continue the attack in a more controlled environment. Using a dedicated, typical endpoint computer, demonstrated the effectiveness of controls with minimal to no “clean up” that typically result of a wide open and reckless phishing campaign.

During the testing of the malicious part of the phishing campaign, we used a controlled, easily reproducible attack which expedited the location of existing effectiveness thresholds of current security controls.

To accomplish the evaluation objectives, we:

- Interviewed key personnel.
- Reviewed documentation to assess security configurations and security control effectiveness.
- Tested system processes to determine the adequacy and effectiveness of selected controls.

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 population was not selected, the results cannot be projected and, if projected, may be misleading.

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Appendix I

Criteria

To perform our evaluation, we used guidance provided by National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, General Services Administration *IT Security Procedural Guide: Conducting Penetration Test Exercises CIO-IT Security-11-51, Revision 5*, and the National Vulnerability Database Common Vulnerability Scoring System Support, *The Common Vulnerability Scoring System*.

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Appendix II

MANAGEMENT COMMENTS

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

FROM: Syed Murshed,
Acting Chief Information Officer

SUBJECT: OIT Response to Request for Comments on the Office of Inspector General Draft Report on the AmeriCorps' Penetration Testing and Phishing Campaign, Report Number: OIG-EV-22-06

DATE: June 30, 2022

AmeriCorps appreciates the opportunity to respond to the Office of Inspector General Draft Report on the AmeriCorps' Penetration Testing and Phishing Campaign, Report Number: OIG-EV-22-06. The OIG has requested that the agency respond, specifying in agreement or disagreement with the findings and recommendations, and providing corrective actions with target implementation dates for each recommendation. With this guidance in mind, the agency's responses, prepared by the Office of Information Technology (OIT) are as follows:

FINDINGS:

Finding #1 - Network Penetration Test (pp. 2-3 of Report): AmeriCorps concurs with the findings regarding OIG's attempt to exploit a vulnerability. As noted in the Report, the agency was able to patch and remediate the potential vulnerability. As also noted, OIT has set up systems to require sufficiently complex passwords as to prevent password cracking via automated or other means.

Finding #2 – Execution of Malicious Code Test (p. 3 of Report): AmeriCorps concurs with the finding that agency systems either blocked or prevented from completion to exploitation level via generation of visible warnings to the user.

Finding #3 – Phishing Campaign (p. 3 of Report): AmeriCorps concurs with the finding that 9 of 85 users receiving a test phishing e-mail ultimately took inappropriate action, despite annual awareness training and additional training for those who fail agency quarterly tests.

RECOMMENDATIONS AND CORRECTIVE ACTIONS

Recommendation 1 (p. 4 of report)

Develop and implement a plan to modify external emails to include information to assist the recipient of the level of risk posed by external email. For example, the Subject line of an email should be modified to identify the source of the email as external to the agency. In addition, the body of the email should contain warnings concerning the dangers of external email and attachments. Finally, warnings should include how frequently the sender has interacted with the recipient.

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Appendix II

The agency agrees with the recommendation.

Corrective Action 1

The agency's Microsoft O365 email system has been re-configured to provide external email tagging. The tags are attached to the beginning of the subject line and included in the message body. OIT commenced testing with a pilot group on June 21, 2022. In addition, OIT has added a new technical policy "AmeriCorps Anti-Phishing Policy" to "Show first contact safety" to address frequency of communication in the Microsoft 365 Security Admin Console. This will show the initial contact with the recipient and warn of infrequent contacts.

Timeline: The SIA (Security Impact Analysis) "Add Caution Tags to emails received from External sources" was approved, and a user communication package was sent agency wide via Gov Delivery on June 27, 2022. OIT anticipates the deployment date for all users in July 2022.

Recommendation 2 (p. 4 of report)

Implement a plan to increase the frequency of behavior training directed at the identification of unwanted spam emails with an emphasis on continual reminders of recognition techniques, appropriate actions, and confidence that self-reporting poor behavioral actions will lead to a better outcome in the future.

The agency agrees with the recommendation.

Corrective Action 2

OIT will roll out an integrated software platform, approved by agency senior management, for security awareness training combined with simulated phishing attack campaigns. The cohesive software tool will deliver the necessary knowledge-based risk mitigation, including recognizing social engineering, spear phishing, and ransomware attacks. As result the agency will increase our accuracy in directing employee knowledge and decision making on security risk in the agency environment.

Timeline: OIT anticipates that operation of the platform will commence in the first quarter of fiscal year 2023.

Recommendation 3 (p. 4 of report)

Implement a process to improve the detection rate to reduce the occurrence of email spam that reaches the users' inboxes.

The agency agrees with the recommendation.

**AMERICORPS
PENETRATION TESTING AND PHISHING CAMPAIGN EVALUATION**

Appendix II

Corrective Action 3

OIT's planned improvements to operational systems includes Microsoft 365 migration which will address this recommendation. Microsoft EOP contains controls to allow for improved detection of e-mail spam.

Timeline: OIT anticipates the completion of this migration by early November 2022.

Syed Murshed
Acting Chief Information Officer

SYED MURSHED  Digitally signed by SYED MURSHED
Date: 2022.06.30 16:41:16 -04'00'



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

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