



Office of Inspector General

Office

202.692.2900

[Website](#)[OIG Reports](#)**Hotline**

202.692.2915 | 800.233.5874

[Hotline](#)OIG@peacecorpsig.gov

To: Paul Shea, Chief Executive Officer, Office of the Director
Emily Haimowitz, Chief Compliance and Risk Officer, Office of the Director

From: Joaquin Ferrao, Inspector General *Joaquin Ferrao*

Date: September 26, 2025

Subject: Special Report on the Peace Corps' Information Technology Environment (IG-25-05-SR)

The Peace Corps' information technology (IT) network and systems contain extensive data and information that are essential to agency operations, including applicant and Volunteer health information and personally identifiable information (PII) of staff and Volunteers. Accordingly, effective controls must exist to prevent unauthorized access to agency systems and sensitive information. The Office of Inspector General (OIG) initiated this review to assess the Peace Corps' IT environment and determine if any vulnerabilities that the agency has not identified exist.

OIG contracted with Singhal & Company, Inc.,¹ to conduct three cybersecurity tests: a penetration test of four critical systems within the Peace Corps' IT environment, a simulated phishing campaign, and a review of the agency's vulnerability management. The tests were conducted from January 2025 to March 2025, in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-115, and other industry standards.

Throughout the assessment, OIG found that the Peace Corps' monitoring capabilities identified the testing activities and demonstrated its incident response procedures. However, the cybersecurity tests also uncovered multiple vulnerabilities and misconfigurations, ranging from informational issues to critical severity risks that the Peace Corps needs to review.

OIG provided a detailed technical report to the Peace Corps that contains sensitive information on the results of this review. This report provides a summary of the penetration test methods that were used and their results. Based on these results, OIG made seven recommendations in this report to support the Peace Corps in strengthening its IT environment, which will better protect its network and data from potential cybersecurity threats and risks. The Peace Corps concurred with all seven recommendations. OIG closed four recommendations (1, 2, 6, and 7) based on the evidence of corrective actions that have already been completed to address the recommendations. The other three recommendations will remain open pending documentation and actions listed in the agency's response. The agency's comments are included in Appendix D, and OIG's response to those comments is in Appendix E. In closing recommendations, OIG is not certifying that OIG has reviewed their effects.

¹ Singhal & Company, Inc. provides IT services and solutions for Government and commercial clients.

PEACE CORPS OFFICE OF INSPECTOR GENERAL

You may address questions regarding follow-up or documentation to the Assistant Inspector General for Audit, David Haney, at 202.692-2958 or dhaney@peacecorpsig.gov.

Please accept OIG's thanks for your cooperation and assistance in our review.

cc: Kris Besch, Deputy Chief Executive Officer, Office of the Director
Richard Swartz, Chief of Staff, Office of the Director
Michael Terry, Chief Information Officer, Office of the Chief Information Officer
Kathryn Wallace, Acting General Counsel, Office of the General Counsel
Clark Presnell, Acting Associate Director, Office of Management
Tracie Hamilton, Acting Chief Financial Officer, Office of the Chief Financial Officer
Devin Meredith, Acting Associate Director, Office of Health Services
Khalid Nayyar, Acting Chief Information Security Officer, Office of the Chief Information Officer
Brian Fauls, Acting Associate Director, Office of External Affairs
Julie Nelson, Compliance Officer Audit Liaison, Office of the Director

ABOUT THIS REPORT

WHY OIG CONDUCTED THIS REVIEW

The Peace Corps' IT network and systems house extensive data and information that are essential to agency operations, including applicant and Volunteer health information and staff and Volunteer PII records. Accordingly, the agency needs to have effective controls in place to prevent unauthorized access to the agency's systems and sensitive information.

The Federal Information Security Modernization Act of 2014² (FISMA) requires Federal agencies, including Peace Corps, to develop, document, and implement agencywide programs that provide cybersecurity for the information and systems that support agency operations and assets. FISMA also requires inspectors general to perform annual independent reviews of their respective agency's information security program and practices. Because the annual FISMA review does not include penetration testing of systems or network security, OIG undertook this review to further assess the Peace Corps' IT environment and determine if any unidentified vulnerabilities exist.

HOW OIG CONDUCTED THIS REVIEW

An organization can assess its IT environment and the effectiveness of its controls through a penetration test; a process in which trusted individuals use common cyber threat actor attack methods to identify network vulnerabilities. OIG contracted with Singhal & Company, Inc., to conduct three cybersecurity tests: a penetration test that targeted critical Peace Corps systems, a simulated phishing campaign, and a review of the agency's internal vulnerability assessment practices. The testing team established agreed-upon rules of engagement with each system stakeholder before the penetration tests were conducted.

The scope of work included penetration testing conducted from two different perspectives: one as a user who has access to the Peace Corps' network (internal testing) and another as an individual who does not have access to Peace Corps' network (external testing). The contractor's testing team conducted penetration tests on four critical systems on the Peace Corps' network.

The vulnerability assessment evaluated the effectiveness of the Peace Corps' security controls by analyzing their vulnerability scanning and management, and phishing defense mechanisms. This part of the testing examined the Peace Corps Office of the Chief Information Officer's (OCIO) procedures for conducting vulnerability assessments on selected systems and applications.

The testing also included a simulated phishing campaign, which sent falsified and fake emails from a location outside of the agency's network to a sample of Peace Corps network users. The fake emails contained a link that recorded how many individuals clicked on it. Links included in real phishing emails often trigger harmful programs to steal information, slow down the network, or cause additional damage to the agency's network and information.

All cybersecurity tests were conducted from January 2025 to March 2025 and were in accordance with the NIST Special Publication 800-115, and other industry standards. Based on the penetration testing results and assessments, the testing team issued a risk rating for each identified vulnerability and an overall risk rating for each system. The ratings represent the

² FISMA, 44 U.S.C. § 3541 et seq.

ABOUT THIS REPORT

magnitude or severity of the risks, which correspond to the potential damage that each risk could cause to the network, ranging from a critical severity risk (highest) to an informational severity risk (lowest).³ These ratings are intended to help the agency prioritize its cybersecurity risks and allocate its limited resources to mitigate the risks with higher severity ratings.

Additional information on how the testing and assessments were conducted is provided in Appendix A. Additional background information on cybersecurity challenges is provided in Appendix B.

BACKGROUND

Protecting agency data and securing information systems is critical across the Government, including at the Peace Corps, which is a global organization comprised of both domestic offices and overseas posts.⁴ The agency manages IT infrastructures for its domestic headquarters in Washington, D.C. and for approximately 57 posts spread geographically across five continents. The network supports more than 3,300 Volunteers who require a variety of resources—including IT capabilities—to meet their performance goals.

Between 2022 and 2023, the Peace Corps experienced three cybersecurity breaches. OIG identified and issued the Management Advisory Report: Cybersecurity Breaches Highlight a Need for Improvement in Peace Corps' Incident Response ([IG-24-01-SR](#)) in December 2023, which reviewed the agency's response to these three cybersecurity breaches. While the agency has since improved its cybersecurity program and increased its FISMA ratings in several areas, as noted in OIG's Review of the Peace Corps' Information Security Program for FY 2024 ([IG-25-01-SR](#)), the agency needs to further strengthen its cybersecurity program.

According to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), cyberattacks are evolving and becoming increasingly complex and harder to detect.⁵ If a cyberattack targeted the Peace Corps and resulted in system outages and data loss, it could have a catastrophic impact on the agency by compromising Volunteer safety, interfering with staff productivity, and negatively affecting the Peace Corps' reputation.

WHAT OIG FOUND

While observing the agency's security processes throughout the assessment, OIG found that the Peace Corps' monitoring capabilities identified the testing activities and demonstrated its incident response procedures. However, the cybersecurity tests also revealed multiple vulnerabilities and misconfigurations ranging from informational issues to critical-severity risks. Overall, the Peace Corps needs to review this report summary in conjunction with OIG's more detailed technical report to determine which risks to prioritize and mitigate to limit potential cybersecurity threats.

³ For a detailed list of the vulnerability levels, see Appendix A.

⁴ For more detail, see the report referenced in Appendix B.

⁵ For more detail, see the CISA webpage on cyberthreats at <https://www.cisa.gov/topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>.

ABOUT THIS REPORT

Since the testing results and findings were communicated throughout this review, the Peace Corps OCIO and other agency leaders have already made progress on the issues identified during OIG's review. For example, the agency started to document, track, address, and mitigate the risks identified in the following sections of this review summary. By addressing these identified vulnerabilities, in conjunction with validating that its systems and tools are properly configured and functioning, the Peace Corp will be able to realize the intended benefits of this review and continue to enhance its IT environment.

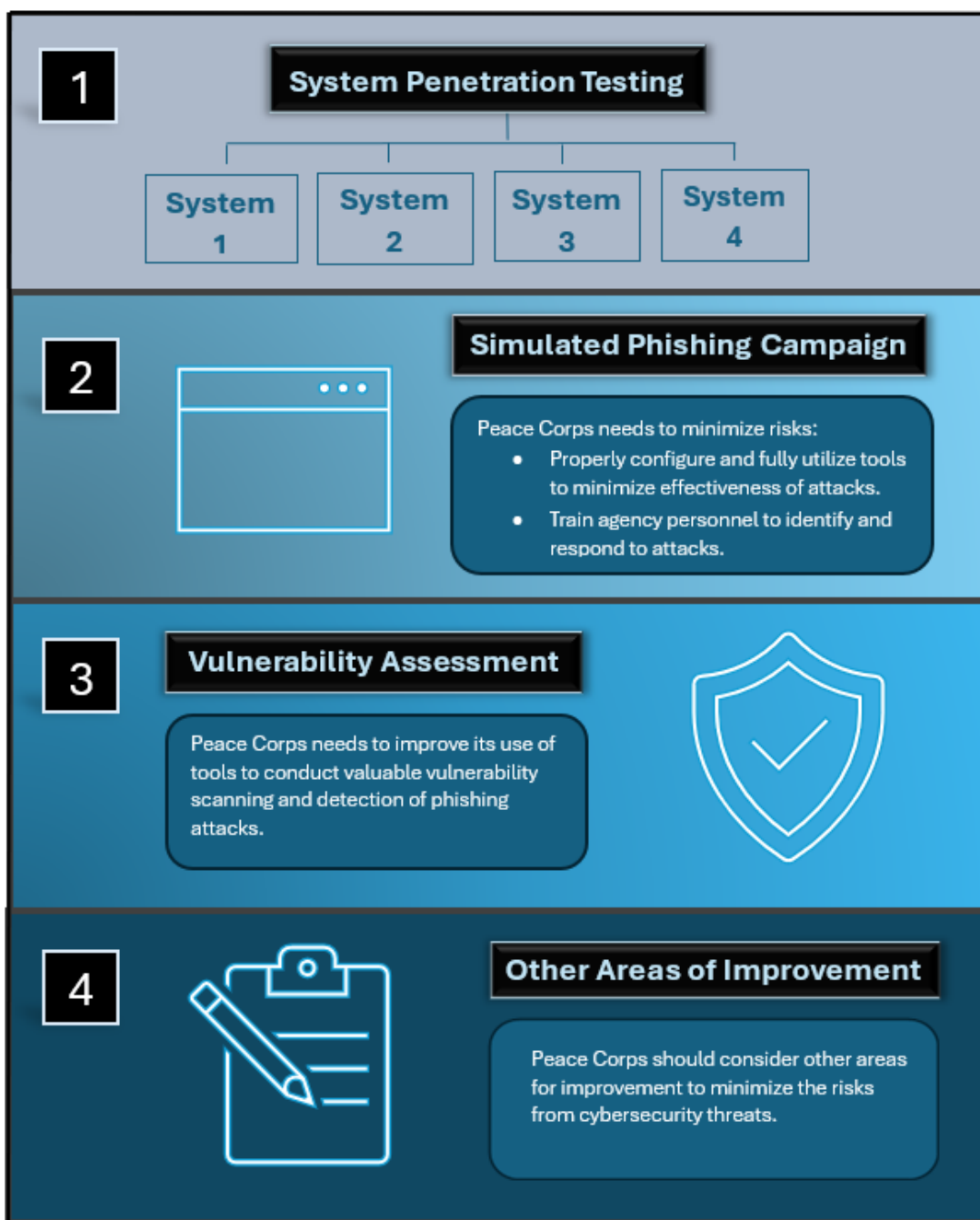
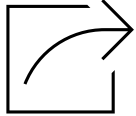


Figure 1: Testing Review Framework

System Penetration Testing



PART 1 - SYSTEM PENETRATION TESTING

OIG tested four critical systems on the Peace Corps' network to identify any vulnerabilities or misconfigurations ranging from informational to critical-severity risks. The penetration tests were intended to provide the system stakeholders with the information necessary to address cybersecurity issues, prevent potential data exploitation, and strengthen the Peace Corps' cybersecurity posture.

WHAT OIG FOUND

Throughout the assessment, the system stakeholders proactively engaged with the testing team during the planning phase of their respective system's penetration tests. During the testing phase, Peace Corps' monitoring capabilities successfully flagged multiple penetration testing activities and other simulated threats. Additionally, the system stakeholders demonstrated effective incident response measures by promptly detecting and investigating these events.

However, the testing team identified multiple vulnerabilities and misconfigurations from critical-severity to informational risks. The testing team determined an overall risk rating of each system based on their review and assessment of the system. A summary of the four systems and their risk ratings is provided below. Additional details and information on each system's identified vulnerabilities and suggested remediations are included in OIG's more detailed technical report. By promptly addressing these identified issues, the Peace Corps will be able to prevent potential cybersecurity threats moving forward while strengthening its overall security posture.

1. System 1

Overall Rating: **Critical**

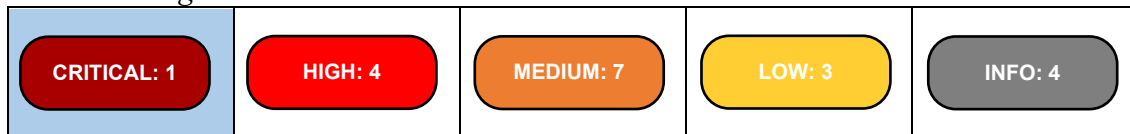


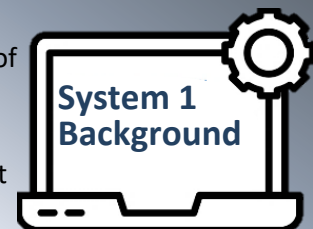
Figure 2: System 1 Vulnerability Ratings

Note: Number of vulnerabilities distribution by severity. Overall rating is highlighted in blue.

System 1 has a **CRITICAL RATING** for its overall security risk rating, primarily because the testing team found that regular domain users had unauthorized access to multiple locations in the system and information on the network. As a result, various data points were exposed, to include sensitive files, PII, personal user folders and files, and other sensitive information. Restricting access to network shares and auditing their contents will prevent potential data breaches and unauthorized information disclosure.

System 1 is a collection of platforms and systems that form a networked infrastructure to support the Peace Corps' data

processing needs. This infrastructure has the most expansive use across the agency's global operations and number of supported users, making it more susceptible to greater vulnerabilities due to its scale and complexity.



System Penetration Testing

Accessible network shares are folders or drives that are made available for use by one or more users. They create a "shared drive" on one network, where employees can access and collaborate on the same files. These shares allow users to access files and resources from other devices without needing to physically transfer or electronically transmitting them. Public shares create risks posed by employees, contractors, or partners who could misuse their authorized access to compromise sensitive data, networks, or systems. These threats can be intentional or unintentional, like accidental data leaks due to negligence or a lack of awareness.

The agency should take immediate action to restrict access to the shares by conducting a thorough audit of their contents and implementing stronger access controls to prevent potential data breaches and unauthorized information disclosures. To effectively manage accessible network shares, the agency should focus on a layered approach that combines share-level permissions and New Technology File System (NTFS) permissions. The agency can set share permissions that allow access for all authenticated users, then use NTFS permissions to grant additional access levels to specific authorized users or groups. This approach ensures granular control over the various access levels while simplifying access management, providing individuals with appropriate access rights, and auditing user access regularly.

In addition, the agency can use security groups, rather than individual users, for permission assignments and enable logging and monitoring to track access and changes. Managing access to shares is a complex issue that requires timely and deliberate policy and systematic implementation. An immediate step that can be taken to prevent unauthorized access to shares within Windows is to disable network discovery and use Group Policy to implement network access restrictions and settings.

2. System 2

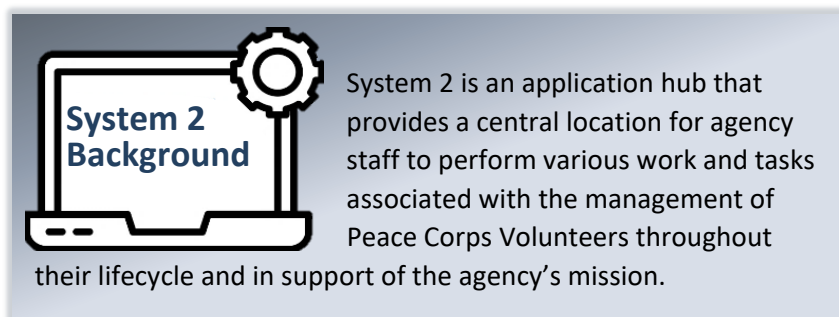
Rating: **Medium**



Figure 3: System 2 Vulnerability Ratings

Note: Number of vulnerabilities distribution by severity. Overall rating is highlighted in blue.

System 2 has a **MEDIUM RATING** for its overall security risk rating. Based on the vulnerabilities identified, the agency should focus on strengthening authentication requirements, restricting access, securing communications, disabling access, and other low or informational risk findings.



System Penetration Testing

3. System 3

Rating: **Medium**

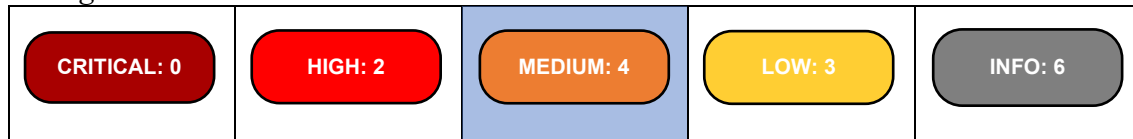
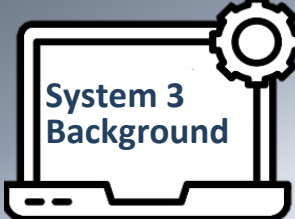


Figure 4: System 3 Vulnerability Ratings

Note: Number of vulnerabilities distribution by severity. Overall system rating is highlighted in blue.

System 3 has a **MEDIUM RATING** for its overall security risk rating. Based on the vulnerabilities identified, the agency should focus on validating and restricting external interactions, updating to the latest versions, restricting permissions and access, securing communications, disabling or restricting access, and other low or informational risk findings.



System 3 Background

System 3 is a financial management application system that accounts for the Peace Corps' business processes and supports the agency's headquarters and overseas posts.

4. System 4

Rating: **Medium**

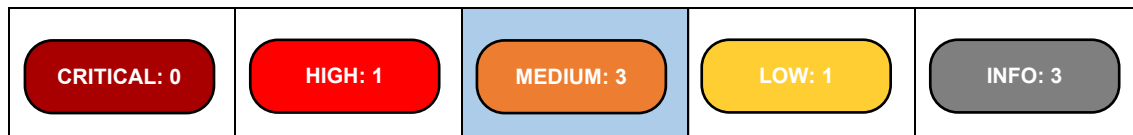
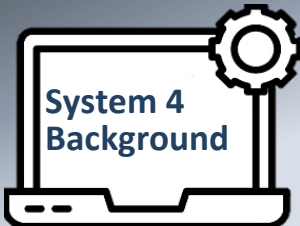


Figure 5: System 4 Vulnerability Ratings

Note: Number of vulnerabilities distribution by severity. Overall rating is highlighted in blue.



System 4 Background

System 4 is a cloud-based solution to manage Volunteer medical information.

System 4 has a **MEDIUM RATING** for its overall security risk rating. Based on the vulnerabilities identified, the agency should focus on properly configuring servers, restricting access, securing communications, disabling access, and other low or informational risk findings.

Peace Corps Needs to Manage the Risks Associated with the Identified Vulnerabilities.

A Plan of Action and Milestones (POAM) document is a FISMA security mandate⁶ that outlines an action plan for how an organization will address and correct identified security vulnerabilities or weaknesses in its system. A POAM acts as a roadmap for implementing corrective actions and supports the agency's progress toward compliance with cybersecurity standards.

⁶ As required by FISMA, 44 U.S.C. § 3541 *et seq.*

System Penetration Testing

A POAM should be incorporated into a Security Authorization Package to demonstrate that a system is appropriately secured in accordance with its applicable Authorization to Operate. When addressing its cybersecurity vulnerabilities, the agency can: 1) deem the risk “acceptable” and develop a Risk-Based Decision to explain the justification for accepting the risk; or 2) deem the risk “unacceptable” and develop a mitigation strategy (which is documented in the POAM). System owners should use risk-based prioritization when developing a POAM.

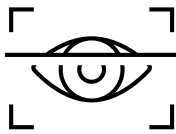
The milestones in each POAM should provide specific descriptions of the steps that will be taken to mitigate the risk. Each POAM needs to have at least one corresponding milestone with an estimated completion date and resource requirements to remediate the risk. POAMs are living documents that should be continually updated as circumstances evolve.

OIG recommends that:

1. The Chief Information Officer reviews the critical-severity vulnerability on System 1 and develop a Plan of Action and Milestones to reduce the threat from accessible network shares.
2. The Chief Information Officer works in coordination with the system owners to review the vulnerabilities identified on each system and develop Plans of Action and Milestones for at least all high-severity vulnerabilities identified above and in the detailed technical report.

Simulated Phishing Campaign

PART 2 - SIMULATED PHISHING CAMPAIGN

 The testing team conducted a simulated phishing campaign on the Peace Corps network and its users to evaluate the Peace Corps' phishing prevention capabilities and response mechanisms, which included targeted phishing simulation exercises and responding system control assessments. This evaluation measured the organization and its personnel's preparedness against email-based attacks and identified potential vulnerabilities in its security posture. The testing results and subsequent assessment provided insights into the effectiveness of the agency's current security awareness training programs and email security infrastructure.



WHAT OIG FOUND

Peace Corps has a Critical Rating for Its Overall Security Risk Rating Related to Phishing Prevention and Response.

The Peace Corps needs to address the weaknesses identified in the areas of:

- configuration and full utilization of network and system tools to minimize the effects of phishing attacks; and
- training agency personnel to identify phishing attacks.

The findings below highlight various risk levels associated with the threat of phishing campaigns, from critical-severity concerns to low-risk observations, based on the analysis of the Peace Corps' anti-phishing measures and existing security controls.

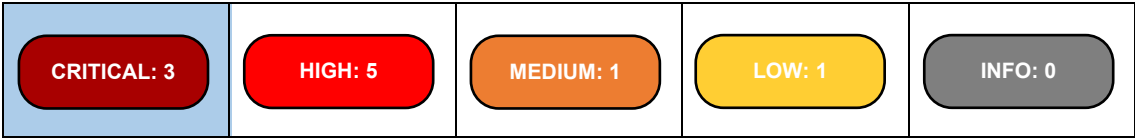


Figure 6: Vulnerabilities Identified During Phishing Campaign

Note: Number of vulnerabilities distribution by severity. Overall rating is highlighted in blue.

Simulated Phishing Campaign

The phishing simulation found that 5.9 percent of the users who received a phishing email clicked on the email links, which, had it been a real phishing attack, could have led to a potential cybersecurity breach. Given that a single click on a corrupted link can compromise entire enterprise systems, every fractional percentage represents the seriousness of this vulnerability. Ideally, the agency's goal should be to have zero clicks during a phishing campaign. OIG recognizes that zero clicks during a phishing campaign may not be attainable, but the IT security program and related training should emphasize the serious threats that phishing campaigns can present and foster a zero click mindset.

Peace Corps Needs to Minimize the Risks Associated with Phishing Attacks.

In many cybersecurity breaches, phishing attacks are often the initial method threat actors use to gain unauthorized access to a network or system. They are incredibly effective due to their low cost, ease of implementation, and offers threat actors the ability to target many individuals with minimal effort. Phishing can lead to significant financial losses, data breaches, and reputational damage for both individuals and organizations. Since a prevalent amount of information is available on social media, threat actors have significant opportunities to use that information to trick users into clicking on a corrupted link during targeted phishing attacks. Artificial intelligence tools are also being used by threat actors to make the false content in phishing emails appear more realistic.

There are multiple actions that the Peace Corps should take to counter the threats of a phishing attack. The recommendations listed below should help the Peace Corps fully use the available system and network tools to protect its network from phishing attacks, ensure Peace Corps personnel are trained to recognize and report on phishing attacks, and improve agency capabilities to reduce the threats from phishing attacks.

OIG recommends that:

3. The Chief Information Officer ensures that the actions shared with the agency in the detailed technical report are taken to properly configure and fully utilize anti-phishing protections.
4. The Chief Information Officer and the Associate Director for Management, review and develop a strategy to provide agencywide training on the phishing reporting process and specific individual training related to those who failed the phishing campaign.
5. The Chief Information Officer implements continuous improvement and emphasize a "Zero Click" mindset throughout the organization to reduce the threat from phishing campaigns.

Vulnerability Assessment

PART 3 - VULNERABILITY ASSESSMENT

The testing team also conducted a vulnerability assessment: a comprehensive evaluation of the organization's current procedures for vulnerability scanning and phishing detection. The main objective of this assessment was to enhance Peace Corps' overall resilience against cybersecurity threats by identifying the strengths, weaknesses, and areas for improvement in its security practices.

WHAT OIG FOUND

The findings below highlight the various risk levels based on the assessment of the Peace Corps' use of tools and its conduct of vulnerability scanning and phishing procedures. Due to the sensitive nature of these results, the details of this assessment have been exclusively provided to the agency in the OIG detailed technical report.

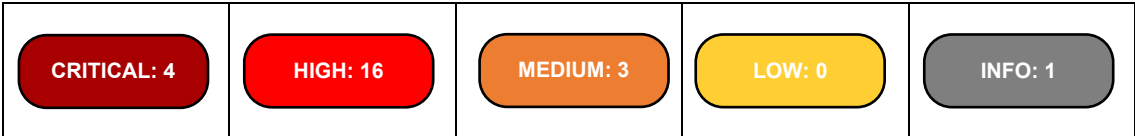
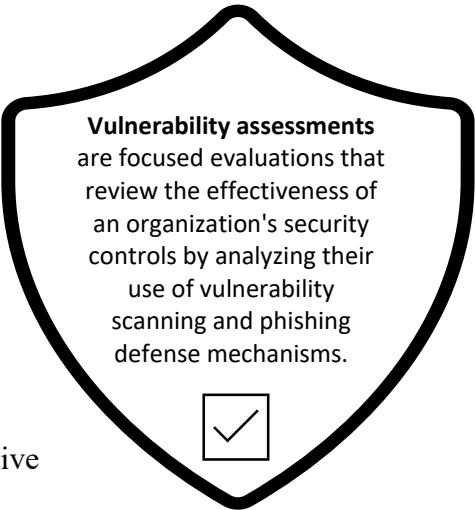


Figure 7: Identified Vulnerability Risk Levels
Note: Number of vulnerabilities distribution by severity.

OIG recommends that:

6. The Chief Information Officer reviews the vulnerabilities identified and develops Plans of Action and Milestones for at least all critical and high-severity vulnerabilities identified in the detailed technical report on the vulnerability assessment.

Other Areas for Improvement

PART 4 - OTHER AREAS FOR IMPROVEMENT

There are additional cybersecurity areas that the Peace Corps can review and consider for improving its operations and minimizing risk.



WHAT OIG FOUND

Like most Federal agencies, the Peace Corps faces numerous cybersecurity challenges, which may include:

- an expanding pool of well-resourced threat actors;
- an increasing number of vulnerabilities resulting from a broad inventory of legacy and new technologies;
- an increasing technology asset inventory and organizational data repository;
- the Peace Corps' global footprint with users and networks operating around the world;
- a lack of resources with exclusive responsibility and ownership of system and data security embedded within each application team;
- an inability to visualize potential harm due to lack of imminent threat;
- limited security resources due to a scarcity of available network tools and environments for testing;
- a lack of separation of responsibility between those finding vulnerabilities and those correcting vulnerabilities;
- routine operational requirements that are prioritized over remediation and correction of known vulnerabilities; and
- budget constraints.

For a more robust security posture, the Peace Corps can build upon the following strengths it demonstrated during this assessment:

- mature policies;
- a well-established governance structure;
- a strong process-based organization structure;
- active stakeholders with a commitment to enterprise security and risk management;
- a strong application of system ownership, systems are working continuously, and access controls;
- no excessive reliance on third party vendors;
- an active mindset toward regulatory compliance; and
- no visible shadow information technology⁷ organization.

⁷ Refers to unauthorized software, hardware, devices, or services without the knowledge or approval of OCIO.

Other Areas for Improvement

Implementing the following recommendations could improve the Peace Corps' cybersecurity posture and reduce the risks from cybersecurity threats.

OIG recommends that:

7. The Peace Corps Director and Chief Information Officer consider the following actions:
 - a. Establish a structured penetration testing program that routinely conducts vulnerability assessment for various systems.
 - b. Manage oversight of Plans of Action and Milestones under a cross functional team which reports to Chief Risk Officer to avoid operational priorities from overtaking remediation activities.
 - c. Establish a matrixed structure where cybersecurity specialists are embedded with each system's Operations and Maintenance team to ensure cybersecurity reviews are an ongoing part of each system opposed to being limited to only a specific milestone, like the Authorization to Operate.
 - d. Utilize cross-training and certification of system stakeholders in cybersecurity practices.
 - e. Establish routine collaboration sessions with Federal partners and trusted vendors focused on cybersecurity experience and best practices to expand knowledge base and best practices while reducing timelines for event monitoring and incident response.

CONCLUSION



During this assessment, the Peace Corps demonstrated security practices, monitoring capabilities, and incident response capabilities. However, the testing also identified multiple vulnerabilities and misconfigurations ranging from informational issues to critical-severity risks that the Peace Corps needs to review. The critical-severity risks identified, particularly during the simulated phishing campaign, need additional focus and attention from the Peace Corps to ensure that they are adequately resolved and reduce the risk of potential cybersecurity threats to the Peace Corps' data and networks that support its operations and Volunteers.

APPENDIX A: SCOPE AND METHODOLOGY

SCOPE

OIG started its planning in October 2024, announced this review in December 2024, and conducted its testing from January 2025 through March 2025. The contractor's testing team conducted external and internal penetration testing on four critical agency information systems in addition to reviewing the Peace Corps OCIO's procedures for conducting vulnerability assessments on selected IT systems and applications. The testing also included a simulated phishing campaign of the Peace Corps' network and users.

METHODOLOGY

The OIG Audit Unit worked with Singhal & Company, Inc. under contract with OIG to complete this review in accordance with NIST Special Publication 800-115 and other industry standards. This review did not follow Generally Accepted Government Auditing Standards.

The testing team used the following structured process to conduct its tests on the Peace Corps' systems and network. The team adhered to the Penetration Testing Execution Standard (PTES), NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, and Open Worldwide Application Security Project (OWASP) Web Security Testing Guide (WSTG) when conducting this review.

TEST PLANNING AND ORGANIZATION

Penetration testing is a process used to identify vulnerabilities and weak misconfigurations that a threat actor could exploit to compromise IT assets and gain unauthorized access to critical information. It tests the resilience of infrastructure against cyberattacks by using the same techniques, tactics, and procedures employed by sophisticated threats.

The test methodology followed five structured phases, each comprised of essential activities that ensure a thorough evaluation.



Figure 8: Test Methodology Phases

All activities were conducted in a manner that simulated the actions of a malicious actor engaging in a targeted attack. The tests were intended to meet the following goals:

- Identify if a malicious actor could compromise critical systems.
- Determine the impact of a security breach on:
 - Confidentiality of private data;
 - Integrity of private data; and

- Availability of information systems.
- Providing recommendations to resolve the security vulnerabilities and misconfigurations addressed to protect against cyberattacks.

Detailed rules of engagement were established for white/gray box testing in accordance with the contractual objectives and in close collaboration with the system owners. By defining and analyzing Peace Corps' network, OIG contractors prepared an attack plan that would fully assess the security of its infrastructure.

ASSESSMENT METHODOLOGY

The assessment followed a comprehensive approach that assessed the system-level attack surface and provided an enterprise-wide view of the IT security posture, specifically identifying and evaluating the risk of exploitable vulnerabilities. During the assessment, different tools and manual testing techniques were used to yield the best results. A few examples of the tools used included, but are not limited to:

- Nmap Scanner
- Nessus/Open VAS
- Metasploit
- Burp Suite
- Wireshark
- Hydra/John the Ripper

The detailed penetration testing methodology followed the five phases of the penetration testing process, with each phase comprised of a set of structured activities. These activities were essential for implementing this assessment, as outlined below:



Figure 9: Penetration Test Methodology Phases

Reconnaissance

The most important phase of any assessment is the reconnaissance—or information-gathering—phase. During this phase, testers identify any information that could be useful in performing a successful attack using Open-Source Intelligence passive and active gathering. This involved hunting for usernames, email addresses, network internet protocol addresses, domains, hosts, services, and web applications, as well as performing an in-depth analysis of the active directory infrastructure, including:

- Domain policies
- Domain privileges

- User and machine account privileges and rights
- Domain and forest trust
- Kerberos services
- Share access
- Groups and organizational units' privileges

Exploitation

The exploitation phase focused on preparing an attack plan to abuse any vulnerabilities and misconfigurations that were discovered. The attack plan consisted of multiple attack paths that could be executed to gain access to the data and systems from both external and internal threats.

Post-exploitation

The post-exploitation phase determined the value of the compromised system; gained the highest amount of control over it using various privilege escalation methods; and finally harvested and exfiltrated any valuable and important data, such as credentials, hashed passwords, and important folders and files.

Pivoting and Lateral Movement

In this phase, the testers used the compromised machines to reach and list other hosts that were not previously accessible to pivot into more internal and hidden networks. Also, by using harvested credentials from compromised systems, the testing team laterally moved and compromised more network hosts of the organization to reach higher-value assets and compromise the entire domain environment.

Reporting and Documentation

The final stage of the test involved creating detailed documentation about the findings, including information on the exploited vulnerabilities, compromised data, how access was achieved and maintained, and corresponding remediation of identified vulnerabilities.

RISK RATING

A risk rating represents the magnitude or severity of that risk. It is based on factors such as the likelihood of occurrence, the potential impact or harm, and the effectiveness of existing controls.

Risk ratings serve as a crucial tool in risk management, allowing organizations to prioritize their systems' risks and allocate their resources to more effectively mitigate those with higher ratings. These rating guide decision-making by providing a standardized way to compare and evaluate various risks within a system, process, or project, facilitating a more strategic approach to risk mitigation.






Severity	Description
 (9.0 - 10.0)	<p>Exploitation of the vulnerability is likely to be straightforward and does not require any special knowledge. It is probably easy to exploit and may result in the attacker gaining full access to the victim's machine with elevated privileges.</p> <p>Such vulnerabilities are a priority during remediation as they pose the highest risk to the confidentiality, integrity, and availability of systems and data.</p>
 (7.0 - 8.9)	<p>Exploitation of the vulnerability is usually more difficult than critical vulnerabilities, but it will still lead to access to the victim machine with elevated privileges which may result in the disclosure of sensitive information or damage and downtime to the agency's systems.</p>
 (4.0 - 6.9)	<p>Vulnerabilities considered to be medium are usually either very hard to set up for and conduct or only result in limited access and control of the victim' machine.</p> <p>Vulnerabilities may require special conditions for them to work such as misconfigured software or user privileges.</p>
 (0.1 - 3.9)	<p>Vulnerabilities categorized as low usually have minimal impact on an organization's systems and flow of work. Exploitation of such vulnerabilities will either yield in minor issues or will require very intricate setup in order to be performed.</p>
 (0.0 - 0.0)	<p>Vulnerabilities categorized as informational usually have no impact on an organization's systems. These are informational findings with negligible risk but can provide attackers with additional information about the operational environment. Remediation is recommended as best practice.</p>

Figure 10: Vulnerability Rating Definitions

APPENDIX B: CYBERSECURITY AS A NATIONAL CHALLENGE

The reliability of computerized data and the systems that process, maintain, and report essential information are a major concern to Federal agencies, the Congress, and the public who rely on computer-based information systems. This dependence on technology provides opportunities for threat actors to cause damage to networks and systems. The U.S. Government Accountability Office (GAO) published a report, *Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231,⁸ which summarized the four major cybersecurity challenges that the Federal Government needed to address:

1. establishing a comprehensive cybersecurity strategy and performing effective oversight;
2. securing Federal systems and information;
3. protecting the cybersecurity of critical infrastructure; and
4. protecting privacy and sensitive data.

Within these 4 challenges there are 10 essential actions to successfully deal with the serious cybersecurity threats facing the nation, as outlined in Figure 11.

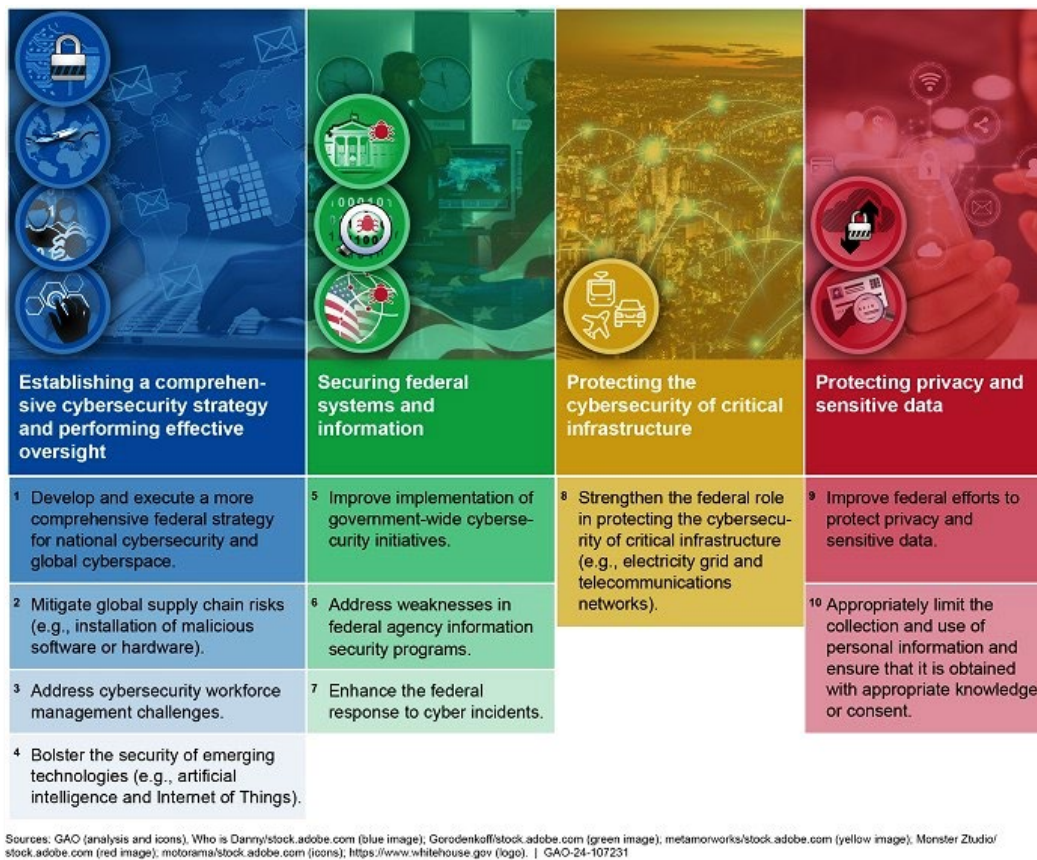


Figure 11: Excerpt from GAO Cybersecurity Report

⁸ <https://www.gao.gov/products/gao-24-107231>, GAO report published June 13, 2024.

APPENDIX C: LIST OF RECOMMENDATIONS

1. The Chief Information Officer reviews the critical-severity vulnerability on System 1 and develop a Plan of Action and Milestones to reduce the threat from accessible network shares.
2. The Chief Information Officer works in coordination with the system owners to review the vulnerabilities identified on each system and develop Plans of Action and Milestones for at least all high-severity vulnerabilities identified above and in the detailed technical report.
3. The Chief Information Officer ensures that the actions shared with the agency in the detailed technical report are taken to properly configure and fully utilize anti-phishing protections.
4. The Chief Information Officer and the Associate Director for Management, review and develop a strategy to provide agencywide training on the phishing reporting process and specific individual training related to those who failed the phishing campaign.
5. The Chief Information Officer implements continuous improvement and emphasize a “Zero Click” mindset throughout the organization to reduce the threat from phishing campaigns.
6. The Chief Information Officer reviews the vulnerabilities identified and develops Plans of Action and Milestones for at least all critical and high-severity vulnerabilities identified in the detailed technical report on the vulnerability assessment.
7. The Peace Corps Director and Chief Information Officer consider the following actions:
 - a. Establish a structured penetration testing program that routinely conducts vulnerability assessments for various systems.
 - b. Manage oversight of Plans of Action and Milestones under a cross functional team which reports to Chief Risk Officer to avoid operational priorities from overtaking remediation activities.
 - c. Establish a matrixed structure where cybersecurity specialists are embedded with each system’s Operations and Maintenance team to ensure cybersecurity reviews are an ongoing part of each system opposed to being limited to only a specific milestone, like the Authorization to Operate.
 - d. Utilize cross-training and certification of system stakeholders in cybersecurity practices.
 - e. Establish routine collaboration sessions with Federal partners and trusted vendors focused on cybersecurity experience and best practices to expand knowledge base and best practices while reducing timelines for event monitoring and incident response.

APPENDIX D: AGENCY RESPONSE



MEMORANDUM

TO: Joaquin Ferrao, Inspector General

FROM: Paul Shea, Chief Executive Officer

PAUL SHEA

Digitally signed by PAUL
SHEA
Date: 2025.09.25
09:55:54 -0400

CC: Kris Besch, Deputy Chief Executive Officer
Richard Swartz, Chief of Staff
Michael Terry, Chief Information Officer
Khalid Nayyar, Acting Chief Information Security Officer
Tracie Hamilton, Acting Chief Financial Officer
Devin Meredith, Acting Associate Director, Office of Health Services
Emily Haimowitz, Chief Compliance and Risk Officer
Kathryn Wallace, Acting General Counsel
Jennifer Piorkowski, Director, Executive Secretariat
Julie Nelson, Compliance Officer, Audit Liaison

DATE: September 26, 2025

RE: Agency Response to the Special Report on the Peace Corps' Information
Technology Environment

Thank you for the opportunity to respond to this preliminary report from the Office of Inspector General (OIG). Enclosed please find the agency's response to the recommendations made by the Inspector General as outlined in the OIG's Special Report on the Peace Corps' Information Technology Environment sent to the agency on August 27, 2025.

Recommendation 1

The Chief Information Officer reviews the critical-severity vulnerability on System 1 and develops a Plan of Actions and Milestones to reduce the threat from accessible network shares.

Concur

Response: The Office of the Chief Information Officer (OCIO) developed a Plan of Actions and Milestones (POAM) for the critical-severity vulnerability on System 1 identified by the OIG.

Documents Submitted:

- POAM for critical-severity vulnerability noted on System 1

Status and Timeline for Completion: September 2025

Recommendation 2

The Chief Information Officer works in coordination with the system owners to review the vulnerabilities identified on each system and develop Plans of Actions and Milestones for at least all high-severity vulnerabilities identified above and in the detailed technical report.

Concur

Response: In collaboration with the system owners, OCIO developed POAMs for the high-severity vulnerabilities identified by the OIG across all systems.

Documents Submitted:

- POAMs for all high-severity vulnerabilities

Status and Timeline for Completion: September 2025

Recommendation 3

The Chief Information Officer ensures that the actions shared with the agency in the detailed technical report are taken to properly configure and fully utilize anti-phishing protections.

Concur

Response: OCIO has reviewed the phishing assessment conducted by the OIG, including parameters related to detection, filtering, gaps, delays, and the response process. Accordingly, POAMs have been created for all items related to the configuring of anti-phishing protections. OCIO will take steps to implement the actions outlined in the POAMs.

Documents to be Submitted:

- POAMs for all phishing related vulnerabilities
- Documentation to verify implementation

Status and Timeline for Completion: January 2026

Recommendation 4

The Chief Information Officer and the Associate Director for Management, review and develop a strategy to provide agency-wide training on the phishing reporting process and specific individual training related to those who failed the phishing campaign.

Concur

Response: The agency concurs with the recommendation to develop a strategy to provide agency-wide training on the phishing reporting process and specific individual training related to those who failed the phishing campaign. The agency maintains an organization-wide cybersecurity awareness training program that covers phishing awareness and other security topics. The following corrective actions will be implemented to strengthen phishing awareness and reporting practices:

1. Dedicated Phishing Reporting Module in the Peace Corps Cybersecurity Awareness Training
2. Agency-Wide Communication and Reinforcement
3. Internal Phishing Campaigns
4. Targeted Remedial Training

Documents to be Submitted:

- Agency-Wide Phishing Report Strategy

Status and Timeline for Completion: December 2025

Recommendation 5

The Chief Information Officer implements continuous improvement and emphasize a "Zero Click" mindset throughout the organization to reduce the threat from phishing campaigns.

Concur

Response: The agency concurs with the OIG's recommendation and will work to actively advance both a "Zero Click" mindset and a culture of continuous improvement to mitigate phishing threats. The agency is confident that the implementation of the Agency Wide Phishing Report Strategy noted in the response to recommendation 4 will directly address the OIG's recommendation, significantly enhance the agency's resilience to phishing attacks, and foster a stronger culture of cybersecurity awareness across the agency.

Documents to be Submitted:

- Agency Wide Phishing Report Strategy

Status and Timeline for Completion: December 2025

Recommendation 6

The Chief Information Officer reviews the vulnerabilities identified and develops Plans of Actions and Milestones for at least all critical and high-severity vulnerabilities identified in the detailed technical report on the vulnerability assessment.

Concur

Response: OCIO developed POAMs for all critical and high-severity vulnerabilities identified in the detailed technical report on the vulnerability assessment.

Documents Submitted:

- POAMs for all critical and high-severity vulnerabilities

Status and Timeline for Completion: September 2025

Recommendation 7

The Peace Corps Director and Chief Information Officer consider the following actions:

- a. Establish a structured pen testing program that routinely conducts vulnerability assessment for various systems.
- b. Manage oversight of Plans of Action and Milestones under a cross functional team which reports to Chief Risk Officer to avoid operational priorities from overtaking remediation activities.
- c. Establish a matrixed structure where cybersecurity specialists are embedded with each system's Operations and Maintenance team to ensure cybersecurity reviews are an ongoing part of each system opposed to being limited to only a specific milestone, like the Authorization to Operate.
- d. Utilize cross-training and certification of system stakeholders in cybersecurity practices.
- e. Establish routine collaboration sessions with Federal partners and trusted vendors focused on cybersecurity experience and best practices to expand knowledge base and best practices while reducing timelines for event monitoring and incident response.

Concur

Response: OCIO is committed to continuous improvement and helping to minimize the risks from cybersecurity threats. The Peace Corps has considered the actions outlined above and created a memorandum outlining the agency's reflections and plans for implementation.

Documents Submitted:

- Memorandum outlining above considerations

Status and Timeline for Completion: September 2025

APPENDIX E: OIG COMMENTS

OIG is encouraged that the agency has concurred with all recommendations in this report. OIG also appreciates the dedication and cooperation of the OCIO and other agency staff managing Peace Corps IT systems. The Peace Corps can greatly improve its IT environment by ensuring that the actions taken and planned in response to this report are completed in a timely manner, which will better protect its network and data from potential cybersecurity threats and risks.

OIG has reviewed the information the agency submitted and has agreed to close recommendations 1, 2, 6, and 7 based on actions taken by the OCIO and the Peace Corps' system owners. While the creation of Plans of Action and Milestones address the vulnerabilities identified and act as an important first step, they do not reduce the risk of these vulnerabilities. The agency must ensure that the plans are effectively implemented, with follow-up actions taken to minimize the risks associated with identified vulnerabilities. Critical and high vulnerabilities should be prioritized and addressed as quickly as possible, as they pose the greatest risk to the agency's information systems.

OIG also notes the importance of allocating sufficient resources to support the execution of these plans. It is critical that corrective actions receive appropriate time, attention, and resources to ensure they are effectively and fully implemented.