To: Carol Spahn, Director.
Emily Haimowitz, Chief Compliance Officer

From: Joaquin Ferrao, Inspector General

Date: December 19, 2023

Subject: Management Advisory Report: Cybersecurity Breaches Highlight a Need for Improvement in Peace Corps' Incident Response

---

The purpose of this report is to bring to your attention needed improvements that the Office of Inspector General (OIG) identified while reviewing Peace Corps' response process for cybersecurity incidents and its adherence to Federal and agency requirements. We reviewed the agency's actions taken during three separate cybersecurity incidents from June 2022 through July 2023.[1]

Our review found that:

- Peace Corps did not have a sufficient incident response plan to detect threat activity, respond to a threat incident, or contain it.
- Peace Corps was not compliant with Federal requirements or Peace Corps' policy for timely notification of cyber breaches.
- Peace Corps' network monitoring software was not effective in detecting malicious activity within the Peace Corps information technology (IT) environment.

To perform this review, OIG analyzed Peace Corps' documentation related to cybersecurity incidents, the National Cybersecurity and Communications Integration Center/U.S. Computer Emergency Readiness Team Federal Incident Notification Guidelines, the National Institute of Standards and Technology (NIST) Special Publication 800-61 Computer Security Incident Handling Guide, the Peace Corps Manual Section (MS) 899, Peace Corps' Breach Notification Response Plan, and prior cybersecurity reports from other Federal Government agencies. OIG also interviewed Peace Corps headquarters staff and external stakeholders, such as Peace Corps' cybersecurity contractors.

Since the first incident in June 2022, the agency has improved its cybersecurity incident response capabilities. However, the agency should continue to improve its incident response program by

[1] OIG conducted this analysis after the first cybersecurity incident investigation concluded in November 2022. While OIG did not perform a full review of the June 2022 and July 2023 incidents, we considered available data in formulating our findings and recommendations.

addressing the findings and recommendations outlined in this report, which includes establishing a more effective response process for future cybersecurity incidents.

Our report makes seven recommendations to help the agency enhance its incident response program. The agency response to the report is included in Appendix B.

BACKGROUND

According to the Cybersecurity and Infrastructure Security Agency (CISA), [2] cyberattacks are evolving by becoming increasingly complex and harder to detect. Cyber incidents can cause harm to national security interests, foreign relations, and the United States economy and civil liberties. As a result, all organizations and individuals should have comprehensive cyber incident detection, response, and prevention strategies. It is critical for Federal agencies, including the Peace Corps, to fully understand the broad range of possible cyber vulnerabilities in their IT infrastructure and obtain the adequate resources needed to detect, respond, contain, and minimize future cyber incidents.

Per CISA, cyberattacks can come in many forms, with malware, phishing, and ransomware becoming more common and affecting both individuals and organizations. Malware is any software that gains unauthorized access to IT systems to steal data, disrupt system services, or damage networks.

To meet these cyberthreat challenges, it is essential that the Peace Corps develops an incident response plan—a written document that helps an agency before, during, and after a confirmed or suspected security incident occurs—to address any cybercrime, data loss, and service outage that threatens its IT environment. Additionally, the Federal Information Security Modernization Act (FISMA) requires Federal agencies to establish such incident response capabilities.

FISMA is designed to ensure that each Federal agency develops, documents, and implements an agency-wide program that provides comprehensive security for the information systems that support their operations and assets. As part of OIG's fiscal year 2023 annual review of the agency's compliance with FISMA, the OIG noted several unresolved issues that had been previously identified in the fiscal year 2022 review, such as:

- an incomplete view of Peace Corps IT environment due to the absence of an up-to-date, accurate, and complete inventory of its information systems, including hardware and software assets;
- an inconsistent implementation of vulnerability and patch management;
- insufficient progress in establishing identity credential and access management program; and
- a lack of a defined enterprise risk management program.

The FISMA review also includes an assessed score that provides a consistent and comparable metric across Government agencies. The five-level scale ranges from Level 1, Ad hoc, to Level 5, Optimized. In fiscal year 2023, the agency maintained a Level 2, Defined, overall rating, as measured against the set of core Federal and supplemental OIG metrics. However, due to the

[2] CISA is an agency within the United States Department of Homeland Security that is responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the Government's cybersecurity protection against private and nation-state hackers.

agency's response to recent cybersecurity incidents, the Peace Corps' Response function was assessed at a Level 1, Ad hoc[3] rating.

The key to mitigating subsequent compromises is to understand potential threats and identify modern attacks in their early stages. In addition, proactively sharing information among organizations about the signs of these attacks has become an increasingly effective way to identify them. The NIST incident response life cycle guidance outlines the four steps that each Federal agency should follow to establish an effective incident response program.

1. **Preparation**: establish an organizational incident response and prevention capability that mediates incidents and ensures the systems, networks, and applications are sufficiently secure
2. **Detection and Analysis**: determine whether an incident has occurred and, if so, the type, extent, and magnitude of the problem
3. **Containment, Eradication, and Recovery:**
    a. Containment: limit an incident before it can overwhelm resources or increase damage, as well as develop a tailored remediation strategy
    b. Eradication: eliminate the incident's components, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all exploited vulnerabilities
    c. Recovery*:* restore systems to normal operation, confirming that the systems are functioning correctly, and, if applicable, remediating vulnerabilities to prevent similar incidents
4. **Post-Incident Activity**: learn and improve from the incident by conducting a lessons learned meeting, creating a follow-up report for each incident, collecting relevant data that is actionable, and retaining any necessary evidence

At the Peace Corps, the Office of the Chief Information Officer (OCIO) oversees IT security and compliance for the agency's information security program.[4] Specifically, the OCIO is responsible for agency cybersecurity awareness and role-based training; conducting systems assessment and authorization; advising on IT security and risk management; testing systems security; assessing agency infrastructure and operations security vulnerability and patch management; monitoring and reporting enterprise information and systems breaches and incidents; and cybersecurity policy and configuration development.

[3] In the FY 2022 FISMA report, Peace Corps' Respond function was at a level 2.

[4] MS 129, Office of the Chief Information Officer: Organization, Mission, and Functions, section 5.0, outlines the functions supported by OCIO.

WHAT WE FOUND

PEACE CORPS DID NOT HAVE A SUFFICIENT INCIDENT RESPONSE PLAN TO DETECT THREAT ACTIVITIES, RESPOND TO THE THREAT INCIDENT, OR CONTAIN IT

The first cybersecurity breach occurred on June 9, 2022, when a threat actor[5] breached the Peace Corps IT environment by launching a tool that gained persistent access to Peace Corps' impacted server. The next day, the threat actor created a local administrator account on the server and extracted credentials from the Peace Corps system. The extraction compromised Peace Corps' administration account, which allowed the threat actor to move throughout nine Peace Corps IT components,[6] risking exposure to many sensitive agency files.

On July 21, 2022, CISA notified[7] the agency that a threat actor was in the Peace Corps IT environment and had potentially compromised a server. Following the notification from CISA, OCIO examined system data logs, reports, and conducted other system analyses on July 22, 2022, and concluded that they did not observe any irregularities or nefarious activities within the IT network. OCIO later attempted to reduce potential risk by disconnecting one of the Peace Corps servers CISA identified as compromised.

Peace Corps was aware that malware and forensic analysis were needed but could not secure assistance from CISA's incident response team. As a result, the agency had to initiate an emergency procurement action for a third-party cybersecurity contractor to conduct its incident response services and a forensic investigation.

In November 2022, the cybersecurity contractors reported that the threat actor had been in the Peace Corps IT environment for 42 days prior to CISA's notification. The report also noted that on July 24, 2022, the threat actor used a data exfiltration[8] tool on three systems in the Peace Corps IT environment, which could copy files to an external cloud-based storage system. However, the investigation could not confirm whether Peace Corps files were exfiltrated. The threat actor remained in Peace Corps' network until July 24, 2022. The contractor indicated that the threat actor voluntarily exited the Peace Corps IT environment and was not removed by OCIO.

Although CISA warned Peace Corps of the breach on July 21, 2022, OCIO's detection capabilities could not sufficiently identify the threat, which subsequently delayed Peace Corps' response to the attack. At the time of the incident, OCIO lacked adequate expertise in responding

[5] A threat actor, also known as a malicious actor, is any person or organization that intentionally causes harm in the digital sphere. They exploit weaknesses in computers, networks, and systems to carry out disruptive attacks on individuals or organizations.

[6] Six servers, post desktop, domain controller, and a system.

[7] Official CISA updates are used to notify stakeholders about potential and active IT system threats to help guard against the ever-evolving ransomware threat environment. These alerts, current activity reports, analysis reports, and joint statements are geared toward system administrators and other technical staff to bolster their organization's security posture.

[8] NIST.gov defines exfiltration as "an unauthorized transfer of information from an information system."

to cybersecurity incidents and did not have sufficient resources to mitigate or effectively investigate the incident.

OIG noted that the agency's incident response plan was ineffective because OCIO did not comply with NIST incident response life cycle guidance: to establish an organizational incident response and prevention capability (such as a contracting mechanism that can quickly obtain the necessary services) to immediately investigate the security incident. As a result, Peace Corps was delayed in procuring cybersecurity contracting services until August 16, 2022. The contractor started its analysis on or near September 14, 2022, and completed its investigation on November 4, 2022. The investigation was completed 106 days after CISA's initial notification.

Additionally, the agency did not maintain sufficient system logs, which hindered the contractor's investigation. Per NIST guidance 800.61, Perform Event Correlation, "Evidence of an incident may be captured in several logs that each contain different types of data […] Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred." Without adequate data logging, an entity cannot exercise event correlations.

Since Peace Corps data logs were insufficient, the third-party cybersecurity contractor could not perform an event correlation, so the agency could not conclusively determine whether exfiltration had occurred. Since the June 2022 breach, the agency has worked with the third-party cybersecurity contractor to strengthen the Peace Corps incident response program's detection and response mechanisms. Additionally, OCIO obtained software[9] to help detect future cybersecurity attacks. The software effectively detected an unrelated incident that occurred in May 2023 and the agency was able to timely mitigate the threat.

We recommend that the:

1. Office of the Chief Information Officer ensures that the network monitoring software is configured at the appropriate levels to detect and minimize Peace Corps exposure to future cybersecurity attacks.
2. Office of the Chief Information Officer implement adequate data logging in compliance with applicable NIST guidance.
3. Office of the Chief Information Officer establish an effective incident response plan to respond to cybersecurity incidents timely.

PEACE CORPS WAS NOT COMPLIANT WITH FEDERAL REQUIREMENTS AND THE PEACE CORPS POLICY FOR TIMELY NOTIFICATION OF CYBER BREACHES.

Peace Corps did not immediately inform CISA of a potential vulnerability in May 2023; they waited until CISA sent out a notification 3 days later. According to OCIO, Peace Corps received a notification on May 30, 2023, from its third-party cybersecurity contractor about a newly discovered vulnerability within Peace Corps' network. Upon receipt of the message, OCIO

[9] The Peace Corps obtained a software that is platform purpose-built to stop breaches with a unified set of cloud-delivered technologies that prevent all types of attacks — including malware.

initiated a review of Peace Corps' IT system, using the software they had installed after the June 2022 breach, which enabled OCIO to timely detect the new threat.

After further investigation, Peace Corps determined that one server had been compromised and exploited before the threat could be contained. More than 5,100 files were exfiltrated, some of which had personal identifiable information and protected health information. There were no indicators of compromise on the remaining servers, and after the incident all servers received the necessary security patches.

Peace Corps notified CISA about a threat on June 2, 2023. If Peace Corps had notified CISA immediately after it had identified the threat, CISA could have used that information to determine whether to alert other agencies of the potential threat. Because Peace Corps did not notify the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (U.S.-CERT)[10] within an hour of the breach, they were not in compliance with the NCCIC/U.S.-CERT Federal Incident Notification Guidelines.

The NCCIC/U.S.-CERT Federal Incident Notification Guidelines states the following requirement:

> Agencies must report information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised, to the NCCIC/US-CERT with the required data elements, as well as any other available information, **within one hour** of being identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department.

Additionally, Peace Corps was not compliant with Peace Corps MS 899.6.2, Incident Response Report, which states:

> (b) After receiving the Incident Response Report, the Incident Response Coordinator in the Office of the Chief Information Officer will complete the Incident Response Report and forward it to: the Chief Privacy Officer, the Privacy Officer, and the Inspector General. The Incident Response Coordinator should forward the Incident Report to the U.S. Computer Emergency Readiness Team (U.S.-CERT) for external reporting as soon as possible after the first notice of the suspected or confirmed breach.

Despite Peace Corps policy, the agency was non-compliant in providing timely incident response notifications to Peace Corps offices on multiple occasions. The Privacy Office was not notified with an Incident Response Report when the first breach occurred in June 2022. Additionally, OIG was not notified about a second breach that occurred in May 2023.

During the June 2022 breach, the agency acknowledged that the policies and procedures outlined in their incident response plan had not been followed, which resulted in a delayed notification of the incident to the Privacy Office and Office of General Counsel staff. The Privacy Office was not informed of the incident as early as needed to coordinate its breach incident duties. However,

[10] Acting as a government-industry coordination center for day-to-day operational National Security Emergency Preparedness (NS/EP) communications support, the National Coordinating Center for Communications was officially recognized as the Communications Sector Information Sharing and Analysis Center, and later integrated into the NCCIC, a 24-hour coordinated information sharing and incident response capability designed to protect and secure the Nation's cyber infrastructure. The NCCIC and NCC are now implemented as part of the CISA Central hub.

following the June 2022 breach, the agency assessed OCIO's response activities and concluded that there were also communication and transparency issues in its incident response process.

On June 2, 2023, CISA notified Peace Corps that there were significant vulnerabilities within the Peace Corps systems. However, OCIO had already detected the threat 3 days earlier, provided a prompt response, isolated the vulnerability, and conducted a forensic investigation of the cyberthreat to minimize the potential compromise. After receiving CISA's confirmation of the breach, OCIO alerted multiple Peace Corps offices; however, OIG was excluded from the original notification. According to OCIO, this exclusion was an oversight because verbal and informal instructions followed within OCIO resulted in confusion and led to the omission of OIG from the notification process.

As a result, OIG was not notified of the security breach until June 22, 2023, during a breach committee meeting, 20 days after the original notification had been provided to the other offices. It is important to notify OIG since a prompt referral to law enforcement could prevent personal identifiable information from being further compromised and, in some cases, reduce the risk of harm to potentially affected individuals.

We recommend that the:

4. Office of Chief Information Officer implements and updates the agency's cybersecurity incident response plan to align with Manual Section 899 to include the Office of Inspector General and other required offices in breach notifications.
5. Office of Chief Information Officer ensures that the United States Computer Emergency Readiness Team and the Cybersecurity and Infrastructure Security Agency receive timely notification when Peace Corps is aware of a potential cybersecurity incident.

PEACE CORPS' NETWORK MONITORING SOFTWARE WAS NOT EFFECTIVE TO DETECT MALICIOUS ACTIVITY WITHIN THE PEACE CORPS IT ENVIRONMENT.

On July 12, 2023, CISA and the Federal Bureau of Investigations (FBI) released a joint Cybersecurity Advisory on enhancing Federal agencies' monitoring of the Microsoft Exchange Online environment to detect malicious activity.[11] Organizations that identify suspicious, irregular activity are instructed to first contact Microsoft to proceed with mitigation actions and then report the incident response activity to CISA and the FBI. According to OCIO, Peace Corps was not affected by this advisory.

However, OCIO investigated whether a breach occurred within Peace Corps' IT environment after receiving notification from Microsoft Security Incident Response that a threat actor compromised Peace Corps network. OCIO confirmed that a user account was compromised from June 27 to June 29, 2023, and responded with several actions designed to remove the existing threat and strengthen defenses against future exploits of this type. In addition, OCIO continued to review the logs and followed-up with CISA regarding the July 12, 2023, cybersecurity advisory.

[11] Enhanced Monitoring to Detect APT Activity Targeting Outlook Online | CISA.

Since Microsoft 365 incurred breaches throughout multiple government agencies, Microsoft stated that as of September 2023 it would roll out expanded logging defaults. Microsoft Purview Audit customers (Audit Standard) will receive deeper visibility into security data, including detailed logs of email access and more than 30 types of log data previously only available at the Microsoft Purview Audit subscription level (Audit Premium). Commercial and government customers with licenses already using Audit Premium will continue to receive access to all available audit logging events, and additional Audit Premium features will include longer default retention periods and automation support for importing log data into other tools for analysis. By ensuring that Peace Corps properly configures the expanded logging defaults, OCIO will be able to continuously monitor the Peace Corps network to mitigate risks of cyberthreats.

We recommend that the:

6. Office of Chief Information Officer configures the networking monitoring software to use the available logs and better identify indicators of compromise within the Peace Corps IT environment.
7. Office of Chief Information Officer ensures that the Peace Corps network is continuously monitored to mitigate the risk of cyberthreats.

CONCLUSIONS AND RECOMMENDATIONS

The agency has been notified of the weaknesses in OCIO's configuration management of information systems in several FISMA reports. Specifically, the agency has not consistently implemented processes for vulnerability management, patch management, or baseline management. In the fiscal year 2023 FISMA review, OIG identified several high and critical vulnerabilities that were not remediated within the timeframe of the agency's vulnerability management plan. As a result, Peace Corps missed opportunities to mitigate critical vulnerabilities that could have prevented systems from being exploited during the first breach. The contractor investigation report stated that patching and vulnerability management were key points of consideration to reduce risks going forward.

Based on the results of the FISMA reviews for fiscal years 2022 and 2023, the agency's inadequate response processes for past breaches, and interviews with OCIO and senior leadership regarding the multiple cybersecurity breaches, OIG found that Peace Corps' security detection activities and incident response program need improvement. Developing a program for the continuous monitoring of Peace Corps' IT network and ensuring that staff follow the required CISA incident response plans and Peace Corps policy will enable the agency to better detect, respond, and mitigate future cybersecurity incidents.

WE RECOMMEND:

1. Office of the Chief Information Officer ensures that the network monitoring software is configured at the appropriate levels to detect and minimize Peace Corps exposure to future cybersecurity attacks.
2. Office of the Chief Information Officer implement adequate data logging in compliance with applicable NIST guidance.
3. Office of the Chief Information Officer establishes an effective incident response plan to respond to cybersecurity incidents timely.
4. Office of Chief Information Officer implements and updates the agency's cybersecurity incident response plan to align with Manual Section 899 to include the Office of Inspector General and other required offices in breach notifications.
5. Office of Chief Information Officer ensures that the United States Computer Emergency Readiness Team and the Cybersecurity and Infrastructure Security Agency receive proper notification when Peace Corps is aware of a potential cybersecurity incident.
6. Office of Chief Information Officer configures the networking monitoring software to use the available logs and better identify indicators of comprise within the Peace Corps IT environment.
7. Office of Chief Information Officer ensures that the Peace Corps network is continuously monitored to mitigate the risk of cyberthreats.

APPENDIX A: LIST OF ACRONYMS

CISA	Cybersecurity & Infrastructure Security Agency
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Modernization Act of 2014
IT	Information Technology
MS	Manual Section
NCCIC/U.S.-CERT	National Cybersecurity and Communications Integration Center/U.S. Computer Emergency Readiness Team
NIST	National Institute of Standards and Technology
NS/EP	National Security Emergency Preparedness
NCCIC/U.S.-CERT	National Cybersecurity and Communications Integration Center/U.S. Computer Emergency Readiness Team
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

APPENDIX B: AGENCY RESPONSE

MEMORANDUM

To: Joaquin Ferrao, Inspector General

Through: Emily Haimowitz, Chief Compliance and Risk Officer

EMILY HAIMOWITZ Digitally signed by EMILY HAIMOWITZ Date: 2023.12.15 07:38:15 -05'00'
Signature

From: Thomas Peng, Chief of Operations and Administration

Peng, Thomas Digitally signed by Peng, Thomas Date: 2023.12.15 11:04:40 -05'00'
Signature

Date: December 17, 2023

CC: Carol Spahn, Director
Lauren Stephens, Chief of Staff
Joshua Romero, White House Liaison
Ruchi Jain, General Counsel
Michael Terry, Acting Chief Information Officer
Helen Walker, Chief Information Security Officer
Francisco Reinoso, Associate Director, Office of Management
Jay Olin, Supervisory Government Information Specialist
Nigel Williams, Risk Officer
Gregory Yeich, Compliance Officer
David Haney, Assistant Inspector General – Audit

Subject: Management Advisory Report: Cybersecurity Breaches Highlight the Need for Improvement in Peace Corps' Incident Response

Thank you for the opportunity to respond to the exposure draft from the Office of Inspector General. Enclosed please find the agency's response to the recommendations made by the Inspector General as outlined in the OIG's Management Advisory Report: Cybersecurity Breaches Highlight the Need for Improvement in Peace Corps' Incident Response sent to the agency on November 17, 2023.

1. **Office of the Chief Information Officer ensures that the network monitoring software is configured at the appropriate levels to detect and minimize Peace Corps' exposure to future cybersecurity attacks.**

   Concur
   Response:
   Recognizing the importance of cybersecurity, OCIO has implemented several enterprise- wide tools and technologies to detect and prevent security events on component systems to help protect the Peace Corps network communication and data. OCIO uses the following enterprise-wide detection and prevention capabilities:
   - Detection – Detection applications such as Intrusion Detection to identify and generate alerts for potentially malicious traffic.
   - Prevention – Technologies with capabilities such as firewalls that monitor, filter, and control network traffic.

   Documents Submitted:
   - Intrusion Detection Platform Guidance

   Status and Timeline for Completion: December 2023

2. **Office of the Chief Information Officer implements adequate data logging in compliance with applicable NIST guidance.**

   Concur
   Response:
   OCIO recognizes the importance of effective centralized logging as a key initiative to improving the agency's incident-sharing responsibilities. In Fiscal Year 22 (FY22), Peace Corps OCIO began an initiative to significantly enhance logging capabilities, including log retention and management, with a focus on ensuring centralized access and visibility. For example, in FY22, the Peace Corps obtained an agency-wide tool for log investigation and incident remediation efforts. The Peace Corps is in the early stages of prioritizing logging capability, deployment, log collection, and storage decisions in accordance with OMB 21-31.

   Documents Submitted:
   - Zero Trust Project Charter
   - Internal OMB 21-31 Compliance Tracker
   - OMB 21-31 Splunk Implementation

   Status and Timeline for Completion: December 2023

3. **Office of the Chief Information Officer establishes an effective incident response plan to respond to cybersecurity incidents timely.**

Concur
Response:
OCIO has policies and controls in place to establish an effective incident response plan. Specifically, the Peace Corps OCIO has drafted a new Manual Section titled "Cyber Incident Response Plan" (IRP), that requires the agency to establish an incident response plan and policy. Furthermore, the Peace Corps has revamped its Incident Response Plan to better align with the Cybersecurity and Infrastructure Security Agency's (CISA) Incident and Vulnerability Response Playbook and NIST's Incident Response life cycle guidance.

Documents to be Submitted:
- Incident Response Plan
- Manual Section titled Cyber Incident Response Plan

Status and Timeline for Completion: June 2024

4. **Office of the Chief Information Officer implements and updates the agency's cybersecurity incident response plan to align with Manual Section 899 to include the Office of Inspector General and other required offices in breach notifications.**

Concur
Response:
OCIO has revamped its Incident Response Plan to better align with applicable Federal mandates, Peace Corps policy standards, and industry best practices. For example, the OCIO has drafted a new Manual Section titled "Cyber Incident Response Plan" to (1) govern the execution of the Incident Response plan and (2) to align with MS 899: Breach Notification Response Plan, which outlines the agency's breach notification process to include the Office of Inspector General and other required offices.

Documents to be Submitted:
- Incident Response Plan

Status and Timeline for Completion: January 2024

5. **Office of the Chief Information Officer ensures that the United States Computer Emergency Readiness Team and the Cybersecurity and Infrastructure Security Agency receive proper notification when Peace Corps is aware of a potential cybersecurity incident.**

Concur
Response:
OCIO has established reporting guidelines to the United States Computer Emergency Readiness Team (US-CERT) and CISA for timely reporting of suspected or confirmed incidents within the Incident Response Plan.

Documents to be Submitted:
- Incident Response Plan

Status and Timeline for Completion: January 2024

6. **Office of the Chief Information Officer configures the networking monitoring software to use the available logs and better identify indicators of comprise within the Peace Corps IT environment.**

Concur
Response:
The OCIO has implemented sophisticated networking monitoring software within the Peace Corps IT environment, specifically adopting a comprehensive strategy to safeguard the integrity of the Peace Corps Microsoft 365 (MS365) Software as a Service (SaaS) cloud tenant. This initiative harnesses an array of cutting-edge Microsoft 365 tools and services to fortify security measures and proactively identify potential indicators of compromise. Among these tools are robust features such as audit logging, advanced threat detection, the Security and Compliance Center, and the Microsoft FedRAMP platform, complemented by the expertise of the dedicated incident response team.

Documents to be Submitted:
- Microsoft Purview Standard Setup SOP

Status and Timeline for Completion: January 2024

7. **Office of the Chief Information Officer ensures that the Peace Corps network is continuously monitored to mitigate the risk of cyber threats.**

Concur
Response:
The OCIO is steadfast in its commitment to maintaining the security of the Peace Corps network for both on-premise and cloud solutions. Leveraging the comprehensive capabilities of MS365, our approach involves continuous monitoring to proactively identify and mitigate cyber threats. Within the MS365 ecosystem, OCIO capitalizes on advanced features such as continuous audit logging and advanced threat detection. The MS365 platform is a FedRAMPed Government Community Cloud (GCC) solution and comes equipped with a vendor incident response team equipped to swiftly address and mitigate any security incidents that may arise, aligning with our commitment to maintaining a resilient and secure network environment for the Peace Corps.

Documents to be Submitted:

- Security Incident Mgt SOP in MS365

Status and Timeline for Completion: January 2024

APPENDIX C: OIG COMMENTS

Management concurred with all seven recommendations. Seven recommendations remain open. In its response, management described actions it is taking or intends to take to address the issues that prompted each of our recommendations. The agency submitted documentation for recommendations 1 and 2. However OIG will need to conduct additional review and further engage with the Office of Chief Information Officer and Compliance Office before considering closing the recommendations.