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.

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.