Peace Corps Office of
INSPECTOR GENERAL

Final Report
Review of the Peace Corps' Information Security Program

September 2023

WILLIAMS ADLEY

EXECUTIVE SUMMARY

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) provides a comprehensive framework for establishing and ensuring the effectiveness of managerial, operational, and technical controls over information technology (IT) that supports Federal operations and assets and provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce IT security risks to an acceptable level. FISMA requires agency program officials, Chief Information Officers (CIO)s, Chief Information Security Officers (CISO)s, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program.

OBJECTIVE

The objective of this review was to perform an independent assessment of the Peace Corps' information security program, including testing the effectiveness of security controls for a subset of systems as required, for fiscal year 2023[1].

RESULTS IN BRIEF

The results of the FY 2023 FISMA review, which assessed the agency's performance against a government wide maturity model, demonstrate that the Peace Corps was able to maintain a Level 2, Defined overall rating. The agency is still working on addressing several unresolved issues identified in the previous year's review, such as:

- Incomplete view of its IT environment due to the absence of an up-to-date, accurate, and complete inventory of its information systems, including hardware and software assets,
- Inconsistent implementation of vulnerability and patch management,
- Insufficient progress in establishing identity credential and access management program, and
- Lack of a defined enterprise risk management program.

Furthermore, due to the agency's response to recent cyber security incidents, we assessed the Peace Corps at Level 1, Adhoc rating, in the Respond function. In order for the Peace Corps to advance their program to Level 3, Consistently Implemented, the agency will need to demonstrate that their developed policies, procedures, and strategy have been consistently applied and followed throughout their daily operations. This requires all staff members to adopt and maintain an information security-focused mindset when engaging in their day-to-day activities. Creating such a shift requires involvement and dedication from every level of the organization, especially at the executive levels.

[1] The Peace Corps Office of Inspector General contracted accounting and management consulting firm Williams, Adley & Company-DC LLP to perform the assessment of the Peace Corps' compliance with the provisions of FISMA.

We continue to encourage the agency to prioritize implementing and maturing their information security program. Focusing on the challenges and addressing the recommendations will elevate the information security program. Adopting these actions will help foster a sustainable culture that incorporates information security[2] across the agency's business operations. Once the agency integrates information security across all its business operations, the Peace Corps will be able to better identify its information security and organization-wide risks, and thus assess and respond to those risks in a timely manner. This, in turn, will reduce the agency's exposure to targeted attacks and environmental disruptions. This will also ensure that resources are utilized in a proactive manner to prevent and address the weaknesses before they are exploited. The Peace Corps will then be able to achieve an effective information security program.

[2] The terms "information security" and "cybersecurity" are used interchangeably throughout the report and convey the same meaning.

TABLE OF CONTENTS

BACKGROUND

THE PEACE CORPS

The Peace Corps is an independent Federal agency whose mission is to promote world peace and friendship by fulfilling three goals: (1) to help people of interested countries in meeting their need for trained Volunteers; (2) to help promote a better understanding of Americans on the part of the peoples served; and (3) to help promote a better understanding of other peoples on the part of Americans. The Peace Corps was officially established on March 1, 1961.

THE OFFICE OF THE CHIEF INFORMATION OFFICER

The Office of the Chief Information Officer (OCIO) provides global IT services and solutions that enable the Peace Corps to achieve its mission and strategic goals. The agency's global IT infrastructure provides services to a user base of nearly 4,000 full-time and part-time personnel distributed throughout the world. OCIO's IT services affect both domestic Peace Corps staff — located at the Washington, D.C. headquarters and remote locations connected via the Virtual Private Network — and international staff located at the Peace Corps' 60+ posts worldwide.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Through the FISMA,[3] each Federal agency is required to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including information and information systems provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of managerial, operational, and technical controls over information technology that supports Federal operations and assets and provides a mechanism for improved oversight of Federal agency information security programs.

FISMA assigns specific responsibilities for strengthening information system security to all Federal agencies, and special responsibilities to the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Department of Homeland Security (DHS). In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, CIOs, CISOs, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS.

On an annual basis, OMB, in coordination with DHS, provides guidance on reporting categories and questions for meeting the current year's reporting requirements.[4] OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

[3] Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).
[4] For example, OMB Memorandum M-20-04, Nov.2019.

CHANGES TO THE REPORTING METRICS FOR FY 2023

In FY 2022[5], OMB changed the guidance for inspectors general (IGs) on how Federal agencies should be reviewed. A set of "core IG metrics" were established to identify the most important data points. These 20 metrics were chosen because they provide sufficient data to determine the effectiveness of an agency's information security program with a high level of confidence. Additionally, these core metrics focus on aligning the review with Executive Order 14028, "Improving the Nation's Cybersecurity," as well as other recent OMB guidance to agencies on the continued efforts to modernize Federal cybersecurity programs.

On December 2, 2022, the OMB issued Memorandum M-23-03[6] ("Memorandum for the Heads of Executive Departments and Agencies: fiscal year 2023 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2023 FISMA reporting requirements. According to the memorandum, the FY 2023 reporting period presents the first opportunity for an agency Inspector General or independent assessor to evaluate the following group of metrics[7]:

- Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.
- Supplemental Metrics – Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

NIST CYBERSECURITY FRAMEWORK

The IG metrics were developed around NIST's Cybersecurity Framework. This framework provides Federal agencies with a common structure for identifying and managing information security risks across the enterprise and provides guidance for assessing the maturity of controls established to address those risks. The Cybersecurity Framework contains five information security functions:

- **Identify** – The "identify" function requires the development of organizational understanding to manage information security risk to systems, assets, data, and capabilities.
- **Protect** – The "protect" function requires the development and implementation of appropriate safeguards to ensure delivery of critical infrastructure services and sensitive information.
- **Detect** – The "detect" function requires the development and implementation of appropriate activities to identify the occurrence of an information security event.
- **Respond** – The "respond" function requires the development and implementation of appropriate activities to take action regarding a detected information security event.

[5] OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements
[6] OMB M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements
[7] Final FY 2023 - 2024 IG FISMA Reporting Metrics v1.1_0.pdf (cisa.gov)

- **Recover** – The "recover" function requires the development and implementation of appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired because of an information security event.

MATURITY MODEL

IGs are required to assess the effectiveness of information security programs on a five-level maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures.

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

In the context of the maturity models, Level 4, managed and measurable, is considered to be an effective level of security at the domain, function, and overall program level. The Level 4 maturity level is defined as formalized, documented, and consistently implemented policies, procedures, and strategies that include quantitative and qualitative performance measures on the effectiveness of those policies, procedures, and strategies, which are collected across the organization and assessed to make necessary changes.

OBJECTIVE

The objective of this review was to perform an independent assessment of the Peace Corps' information security program, including testing the effectiveness of security controls for a subset of systems as required, for FY 2023[8]. For more information on the methodology used, see Appendix A. For a list of Federal requirements used as criteria, see Appendix D.

[8] The Peace Corps Office of Inspector General contracted accounting and management consulting firm Williams, Adley & Company LLP-DC to perform the assessment of Peace Corps' compliance with the provisions of FISMA.

RESULTS

The results of the FY 2023 FISMA review, which assessed the agency's performance against a government wide maturity model, demonstrate that the Peace Corps was able to maintain a Level 2, Defined overall rating. The agency is still working on addressing several unresolved issues identified in the previous year's review, such as:

- Incomplete view of its IT environment due to the absence of an up-to-date, accurate, and complete inventory of its information systems, including hardware and software assets,
- Inconsistent implementation of vulnerability and patch management,
- Insufficient progress in establishing identity credential and access management program, and
- Lack of a defined enterprise risk management program.

Furthermore, due to the agency's response to recent cyber security incidents, we assessed the Peace Corps at Level 1, Adhoc rating, in the Respond function. In order for the Peace Corps to advance their program to an overall rating Level 3, Consistently Implemented, the agency will need to demonstrate that their developed policies, procedures, and strategy have been consistently applied and followed throughout their daily operations. This requires all staff members to adopt and maintain an information security-focused mindset when engaging in their day-to-day activities. Creating such a shift requires involvement and dedication from every level of the organization, especially at the executive levels.

We continue to encourage the agency to prioritize implementing and maturing their information security program. Focusing on the challenges and addressing the recommendations will elevate the information security program. Adopting these actions will help foster a sustainable culture that incorporates information security[9] across the agency's business operations. Once the agency integrates information security across all its business operations, the Peace Corps will be able to better identify its information security and organization-wide risks, and thus assess and respond to those risks in a timely manner. This, in turn, will reduce the agency's exposure to targeted attacks and environmental disruptions. This will also ensure that resources are utilized in a proactive manner to prevent and address the weaknesses before they are exploited. The Peace Corps will then be able to achieve an effective information security program.

UNRESOLVED CHALLENGES

Despite the agency's efforts to address the concerns identified in the previous year's review, several major unresolved issues persist in the current year, such as the following:

- Incomplete view of its IT environment due to the absence of an up-to-date, accurate, and complete inventory of its information systems, including hardware and software assets,
- Inconsistent implementation of vulnerability and patch management, and

[9] The terms "information security" and "cybersecurity" are used interchangeably throughout the report and convey the same meaning.

- Insufficient progress in establishing an Identity Credential and Access Management (ICAM) program.

Incomplete View of Its IT Environment and Inconsistent Implementation of Vulnerability and Patch Management

The agency has consistently encountered issues related to a lack of visibility into their IT assets. Without a comprehensive inventory, it is difficult to identify all the hardware and software present in the Peace Corps' environment. This lack of awareness leaves gaps in security coverage, as vulnerabilities can go unnoticed. This increases the likelihood of overlooking vulnerabilities that need to be patched or updated, leaving systems exposed to potential attacks.

Inconsistent implementation of vulnerability and patch management can have a range of negative impacts on an organization's cybersecurity and operational effectiveness. Based on the various scan results examined this year, we identified several high and critical vulnerabilities that were not remediated within the timeframe outlined in the Peace Corps process. These unpatched vulnerabilities can create entry points for cybercriminals to breach systems and compromise sensitive data.

Insufficient Progress in Establishing an Identity Credential and Access Management Program

Over the years, the Peace Corps has not finalized an ICAM strategy to guide the agency's ICAM program. The agency has developed an ICAM strategy roadmap in FY 2022 to identify all milestone deliverables required to complete a comprehensive ICAM program, such as:

- Federal Identity, Credential, and Access Management (FICAM) Strategy assessment and implementation,
- Multi-Factor Authentication (MFA) enforcement for domestic and international privileged user accounts, and
- MFA Enforcement for domestic and international non-privileged user accounts.

This year, the Peace Corps has made some progress in meeting the milestones identified in the ICAM roadmap. However, many of the deliverables (policies and procedures) are still in progress and the agency has stated that these will be finalized by the end of calendar year. All project deliverables are expected to be completed by the end of FY 2024 Quarter 2.

These are a few of the unresolved issues that continue to impede Peace Corps commitment to cybersecurity and risk management. The delay of action demonstrates a lack of urgency and accountability in rectifying potential security gaps. Neglecting to address these issues leaves the agency exposed to cyber threats and compromises the integrity of sensitive information. It is crucial for the agency to promptly implement remediation measures to fortify its security posture and safeguard against future risks. Specifically, the Peace Corps needs to prioritize addressing two distinct areas of concern in the upcoming years.

LACK OF AN ESTABLISHED INCIDENT RESPONSE PROCESS

During our FY 2023 review, we became aware of a security incident, where the Peace Corps' incident response team did not identify the potential incident and was notified by the Cybersecurity

and Infrastructure Security Agency (CISA) of access to the network by an unauthorized third-party in the summer of 2022. However, due to a lack of resources and expertise, the Peace Corps' incident review was not thorough in fully analyzing and remediating the potential incident. Through cyber security tools, Peace Corps was notified a month later of several machines affected by a suspicious execution file, tracing back to a malicious IP address. The Peace Corps then contacted CISA and a third party contractor for investigative and remediation assistance. Because of numerous contracting challenges encountered by the agency, the analysis conducted by the third party contractor team could only commence two months after the threat actor gained access into the environment and was ultimately concluded at the end of the 2022 calendar year. The third party contractor report identified the following:

- The earliest evidence of threat actor activity in the Peace Corps environment occurred in early summer of 2022,
- Threat actor executed a utility typically used by threat actors for data exfiltration on three systems in the Peace Corps environment, and
- Threat actor created and leveraged an administrative account for credential harvesting and lateral movement.

Upon discovering this information, the agency acquired additional tools and personnel resources in an effort to address both current and potential issues. Peace Corps closed the incident ticket in the first quarter of 2023 as CISA and the third-party contractor found no conclusive evidence of successful data exfiltration within Peace Corps' environment. However, it is important to note that the threat actor was able to access the system for an extended period of time without being detected. This unauthorized access resulted in the compromise of the system, potentially putting sensitive information at risk of being accessed or stolen by the threat actor. We believe this incident could have been mitigated had the agency possessed sufficient resources, tools, and processes to comprehensively investigate and respond to potential incidents. This incident further highlighted Peace Corps' current inadequate incident response process, such as (a) a lack of centralized definition for "breach" and "major incident" to ensure proper protocol was followed and (b) a lack of guidance on internal reporting timeframe between the OCIO, privacy team, and the Office of the General Counsel (OGC) team to ensure all information is disseminated and all relevant parties are involved.

According to NIST 800-61[10], preparation is the initial phase of incident response process, which includes setting up an incident response team and providing them with proper training, as well as acquiring the necessary tools and resources. This involves establishing a structured incident response capability within the organization, which will enable swift and effective action when incidents occur and contribute to minimizing potential damage and downtime. Without these foundational elements, managing security incidents becomes significantly more difficult. The Peace Corps' absence of preparedness and a well-defined incident response plan not only hampers its ability to respond swiftly and effectively but can also lead to heightened risks, increased damage, and longer recovery times in the event of an incident.

[10] Computer Security Incident Handling Guide (nist.gov)

Furthermore, in our review of the aforementioned incident and another in early summer of 2023[11], we determined that the Peace Corps does not have a defined process to capture, track and maintain its incident logs. Specifically, the Peace Corps does not have a defined process to clearly identify, maintain, and generate the following information:

- Events to be analyzed by the Security Operation Center/Incident Response team,
- Events reportable to the United States Computer Emergency Readiness Team, and
- Events declared as incidents.

Additionally, we were unable to identify all steps taken by the agency to remediate and resolve the incidents. The records maintained within the Track-It! system did not demonstrate that the appropriate procedures outlined in the agency's guidance were taken.

LACK OF A DEFINED ENTERPRISE RISK MANAGEMENT PROGRAM

The Peace Corps has struggled to implement a comprehensive ERM program over the years, which was highlighted as an area of concern in the FY 2022 FISMA report. Despite outlining organizational risk management as one of the agency's key management objectives in their strategic plan starting in FY 2018, the Peace Corps has not fully implemented an ERM program.

The Peace Corps first codified the ERM governance structure in July 2019 with the publication of a Peace Corps Manual Section, an ERM Council Charter, and ERM Council By-laws. The ERM Council was charged with the responsibility to review, evaluate, and monitor opportunities and risks impacting the agency's ability to achieve its mission and strategic objectives. Since its inception, the Council has been convening on an ad-hoc basis and has not yet guided the Peace Corps in its implementation of a comprehensive risk management framework or system. In FY 2023, the Council began to convene quarterly, and on an as-needed basis, to discuss ERM program updates such as office-level and agency-level risk registers, agency risk appetite statement, and agency risk profile. These meetings also serve as a venue for the different offices to discuss critical risks and monitor existing risks.

However, the agency has not yet defined risk tolerance within its ERM policies and procedures, which is a foundation in pursuing an effective information security program. The agency plans to update and republish its existing ERM policies and procedures to align with the current processes by December 2023. Specifically, the Peace Corps plans to finalize the ERM program plan, which will articulate the risk philosophy, architecture, governance, and processes to monitor and communicate risks across all organizational levels. The ERM program plan will be all-inclusive and will integrate information security as well as considering the agency's risk appetite and tolerance.

The delay in improving its ERM program stems from the Peace Corps not dedicating enough resources and/or assigning appropriate personnel to such a crucial initiative. Up until FY 2022, the establishment and implementation of ERM has been handled by a variety of staff members as collateral and part-time duties. To address such gap, as part of the recent budget and strategic

[11] As of the end of our review period, this incident is still under active investigation and remediation.

investments, the Peace Corps has allocated and filled a position of Risk Officer in June 2023 to oversee the ERM program and its progress.

CYBERSECURITY INTEGRATION WITH ERM

Cybersecurity risks could expose the agency to exploitation of vulnerabilities which could lead to compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by an organization's information systems.

ERM programs should ensure cybersecurity risk is given appropriate and sufficient attention due to the increasing frequency, creativity, and severity of cybersecurity attacks. This will allow enterprises and their component organizations to better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.[12]

For ERM purposes, each system and organization should have a cybersecurity risk register that explicitly records and communicates risk decisions considering the enterprise risk strategy. Per OMB Circular A-11, a risk register is described as "a repository of risk information including the data understood about risks over time." It also states that "Typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks." Cybersecurity risk registers are a key aspect of managing cybersecurity risks within an enterprise. Each register evolves and matures as other risk activities take place.

At higher levels of the enterprise, the contents of those registers should be analyzed across all risks and trade-offs when allocating resources or prioritizing decisions based on the metrics established in the ERM program. The use of cybersecurity risk registers provides consistency in capturing and communicating risk-related information (including risk response) throughout the ERM process. It then provides a framework for organizing and communicating risk information from the individual information system level to the business process level and ultimately to the enterprise level. The risk registers used at each level convey information about risk assessments, evaluation decisions, responses, and monitoring activities. They can be used as a formal communication vehicle for sharing and coordinating cybersecurity risk activities as an input to ERM decision makers.

BENEFITS TO AGENCY

Dedicating resources to address the provided recommendations will allow the Peace Corps to cultivate an environment of continuous improvement, paving the way for long-term success.

The agency can better manage and mitigate risks by proactively identifying potential threats and vulnerabilities, making it easier to prevent incidents before they occur. It will also allow the Peace Corps to respond quickly and efficiently to security incidents. The ability to detect, analyze, and contain incidents promptly helps minimize the damage and reduces the overall impact on the business. By investing in incident response preparedness, the Peace Corps can strengthen its security posture and be better equipped to handle the evolving threat landscape.

[12] NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2020

In addition, with a well-defined ERM program that incorporates a comprehensive view of cybersecurity risks, the Peace Corps will be able to gain greater awareness about the risks facing the organization and improve its ability to respond effectively. This will foster an organizational climate where cybersecurity risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes. Establishing the risk guidance at the executive level will help individuals with responsibilities for information system implementation or operation better understand how cybersecurity risks associated with their information systems translates into enterprise-wide risk that may ultimately affect the mission/business success. By setting up a solid foundation for ERM, the Peace Corps can achieve:

- Enhanced confidence about the achievement of strategic objectives,
- Improved compliance with legal, regulatory, and reporting requirements, and
- Increased efficiency and effectiveness of operations.

Focusing on the implementation of ERM principles and separately improving the agency's incident response process, will foster a culture that fully integrates information security into its business operations. This will help the Peace Corps to utilize its resources in a proactive manner to prevent and address the weaknesses before they are exploited. The Peace Corps will then be in a better position to achieve success in implementing an effective information security program.

RECOMMENDATIONS

OIG recommends:

1. The Peace Corps develops a strategy and structure that integrates information security into the agency's business operations. This should include an established responsibility for assessing information security risks in all agency programs and operations and providing this analysis to senior leadership, including the ERM Council, for decision-making.
2. The Peace Corps include the CISO at the ERM Council meetings to provide insights on cybersecurity risks.
3. The Peace Corps further define and implement the ERM program to ensure information security risks are communicated and monitored at the system, business process, and entity levels.
4. The Peace Corps improve its incident response process to ensure incidents are properly defined, promptly identified, and effectively remediated.
5. The Peace Corps consistently improve and implement its inventory management process to ensure information system, hardware, and software inventories are accurate, complete, and up to date.
6. The Peace Corps improve its vulnerability and patch management processes by consistent and timely remediation of critical and high vulnerabilities as well as patching.
7. The Peace Corps complete and fully implement an identity credential and access management program.

APPENDIX A: SCOPE AND METHODOLOGY

FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency's inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to OMB and DHS. The FY 2023 FISMA guidance from DHS is intended to assist OIGs in reporting FISMA performance metrics.

The objective of this review was to perform an independent assessment of the Peace Corps' information security program, including evaluating the effectiveness of security controls for a subset of systems as required, for FY 2023:

- Peace Corps General Support System (PCGSS),
- PC Medical Electronic Documentation & Inventory Control System (PCMEDICS), and
- Peace Corps Security Operations Center (PCSOC).

The Peace Corps OIG contracted accounting and management consulting firm, Williams, Adley & Company LLP-DC (Williams Adley) to perform the assessment of the Peace Corps' compliance with the provisions of FISMA. Williams Adley performed this review from April to July 2023. Williams Adley performed the review in accordance with FISMA, OMB, and NIST guidance.

Williams Adley believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the review objectives. The audit work was performed to meet Government Auditing Standards, 2018 Revision with Technical Update April 2021, the United States Government Accountability Office (GAO)-18-568G, Chapter 3, Ethics, Independence, and Professional Judgement; Chapter 4, Competence and Continuing Professional Education; Chapter 5, Quality Control and Peer Review; and Chapter 8, Fieldwork Standards for Performance Audits.

The following laws, regulations, and policies were used to evaluate the adequacy of the controls in place at the Peace Corps:

- FISMA Inspector General and CIO Metrics (FY 2023-2024)
- Public Law 113–283, FISMA
- OMB Circulars A-123, A-130
- OMB/DHS Memorandums issued annually on Reporting Instructions for FISMA and Agency Privacy Management
    - OMB M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements
- NIST Special Publications (SP) and NIST Federal Information Processing Standard Publications
- Peace Corps' policies and procedures relating to the nine FISMA domains

Williams Adley acknowledges that (a) it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist at all in other information systems that were not tested and (b) it is possible that other deficiencies may exist that are unique to the information systems not included within this review. However, a prudent person without any basis in fact would not automatically assume that these deficiencies are non-existent or existent with other systems. Such a supposition would be especially ill-advised for an issue as important as information security. Williams Adley will evaluate other information systems in subsequent years using rotational multi-year strategy.

APPENDIX B: USE OF COMPUTER PROCESSED DATA

During the review, Williams Adley utilized computer-processed data to obtain samples and information regarding the existence of information security controls. Specifically, Williams Adley obtained data extracted from Microsoft's Active Directory to test user account management controls. Williams Adley also reviewed data generated by software tools to determine the existence of security weaknesses that were identified during vulnerability assessments. Williams Adley assessed the reliability of computer-generated data primarily by comparing selected data with source documents. Williams Adley determined that the information was reliable for assessing the adequacy of related information security controls.

APPENDIX C: LIST OF ACRONYMS

Acronym	Definition
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	U.S. Department of Homeland Security
EO	Executive Order
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
ICAM	Identity Credential and Access Management
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCGSS	Peace Corps General Support System
PCMEDICS	Peace Corps Medical Electronic Documentation & Inventory Control
PCSOC	Peace Corps Security Operations Center

APPENDIX D: GUIDANCE

The following NIST guidance and Federal standards were used to evaluate the Peace Corps' information security program.

I. Identify

a. Risk Management

i. NIST SP 800-37 Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

ii. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and System View*

iii. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*

iv. NIST SP 800-60*, Guide for Mapping Types of Information and Information Systems to Security Categories*

v. Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Security Systems*

vi. DHS Binding Operative and Emergency Directives

vii. OMB Circular A-123, *Management's Responsibility for Internal Control*

viii. OMB Circular A-130, *Managing Information as a Strategic Resource*

ix. NIST IR 8286 Integrating Cybersecurity and Enterprise Risk Management

b. Supply Chain Risk Management

i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*

ii. Federal Acquisition Supply Chain Security Act of 2018

iii. NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

II. Protect

a. Configuration Management

i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*

ii. OMB M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

iii. NIST SP 800-128, *Guide for Security Focused Configuration Management of Information Systems*

iv. OMB M-20-32, *Improving Vulnerability Identification, Management, and Remediation*

b. Identity and Access Management
   i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
   ii. HSPD-12, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*
   iii. NIST SP 800-128, *Guide for Security Focused Configuration Management of Information Systems*
   iv. NIST SP 800-63 *Digital Identity Guidelines*
   v. Federal Identity, Credential, and Access Management (FICAM) Implementation Guidelines
   vi. FIPS 140-2, *Security Requirements for Cryptographic Modules*
   vii. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
   viii. OMB Circular M-19-17, *Enabling Mission Delivery through Improved Identity Credential, and Access Management*

c. Data Protection and Privacy
   i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
   ii. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*
   iii. OMB Circular M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
   iv. OMB M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*
   v. DHS BOD 18-01 *Enhance Email and Web Security*
   vi. DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*
   vii. FY 2023 CIO FISMA Metrics

d. Security and Privacy Training
   i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
   ii. NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
   iii. NIST SP 800-181 *Workforce Framework for Cybersecurity (NICE Framework)*
   iv. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
   v. Workforce Framework for Cybersecurity (NICE Framework)

vi. Federal Cybersecurity Workforce Assessment Act of 2015

III. Detect

a. Information Security Continuous Monitoring

i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*

ii. NIST SP 800-37 Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

iii. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

IV. Respond

a. Incident Response

i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*

ii. CISA Cybersecurity Incident and Vulnerability Response Playbooks

iii. NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*

iv. NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*

V. Recover

a. Contingency Planning

i. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*

ii. NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*

APPENDIX E: AGENCY COMMENTS

MEMORANDUM

To: Joaquin Ferrao, Inspector General

Through: Emily Haimowitz, Chief Compliance and Risk Officer

EMILY HAIMOWITZ Digitally signed by EMILY HAIMOWITZ Date: 2023.09.14 12:23:26 -04'00'
Signature

From: Thomas Peng, Chief of Operations and Administration

Peng, Thomas Digitally signed by Peng, Thomas Date: 2023.09.14 13:33:17 -04'00'
Signature

Date: September 15, 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
Nigel Williams, Risk Officer
Gregory Yeich, Compliance Officer
Renita Davis, Acting Assistant Inspector General – Audit

Subject: Review of the Peace Corps' Information Security Program for FY 2023

Enclosed please find the agency's response to the recommendations made by the Williams Adley auditors and the Inspector General as outlined in the Review of the Peace Corps' Information Security Program for FY 2023 given to the agency on August 25, 2023.

1. **OIG recommends that the Peace Corps develops a strategy and structure that integrates information security into the agency's business operations. This should include an established responsibility for assessing information security risks in all agency programs and operations and providing this analysis to senior leadership, including the ERM Council, for decision-making.**

   Concur

   Response:
   The Peace Corps will develop a strategy and structure that integrates information security into the agency's business operations. Specifically, the strategy will establish responsibility for the assessment of information security risks across all agency programs and operations and will be provided to agency leadership for decision making. In support of this undertaking, the agency has recently approved two additional personnel to the Chief Information Security Officer (CISO) office as Fiscal Year (FY) 24 investments to assist with tactical operations. Until this investment is realized in FY24, current resource constraints primarily limit the CISO to operational and tactical planning with limited focus applied toward strategic development.

   Documents to be Submitted:

   - Enterprise Risk Management (ERM) Program Plan
   - CIO-SEC-PLN-07 Risk Management Strategy

   Status and Timeline for Completion: September 2024

2. **OIG recommends that the Peace Corps include the CISO at the ERM Council meetings to provide insights on cybersecurity risks.**

   Concur

   Response:
   In FY23, the Peace Corps added the CISO to its ERM Secretariat, which is an advisory body that supports the planning and implementation of ERM actions. All ERM Secretariat members are expected to attend the ERM Council meetings. In FY23, the CISO attended all four quarterly ERM Council meetings and the ad hoc meetings to discuss particular time-sensitive risks being raised to the Council.

   The Peace Corps will continue to ensure the CISO is a member of the ERM Secretariat and is included in all ERM Council meetings. The agency will further document the roles and responsibility of the ERM Secretariat in appropriate policy and/or charter.

   Documents to be Submitted:

   - Quarterly ERM Council meeting minutes, including attendance

- Updated policy and/or charter outlining the roles and responsibilities of ERM Secretariat members

Status and Timeline for Completion: March 2024

3. **OIG recommends that the Peace Corps further define and implement the ERM program to ensure information security risks are communicated and monitored at the system, business process, and entity levels.**

Concur

Response: The ERM program implementation elements will continue to develop going forward. The Risk Officer's primary focus in FY24 is the development of an ERM Program Plan, which will serve as an overarching plan geared to enable ERM to implement the agency's risk management mission and vision, and will include risk management landscape considerations. Developments of note in the last quarter of FY 23 that evidence progress toward meeting this recommendation include the adoption of risk management standards, the enhancement of a risk management decision making framework, and the development of the agency's first risk profile. Additionally, the Risk Officer and the CISO have established a monthly meeting cadence to define and implement approaches that meet both the risk management standard and NIST guidance.

Documents to be Submitted

- Enterprise Risk Management (ERM) Program Plan

Status and Timeline for Completion: March 2024

4. **OIG recommends that the Peace Corps improve its incident response process to ensure incidents are properly defined, promptly identified, and effectively remediated.**

Concur

Response:
The Peace Corps will further refine our Automated Tracking and Data Collection process to assist in the tracking of security incidents and collection and analysis of incident information. The Office of the Chief Information Officer (OCIO) intends to remediate the identified weakness through a combination of technical updates and procedural quality control steps. Specifically, OCIO's issue-tracking system will be updated to maintain records about the status of incidents, along with other pertinent information such as summary of the incident, indicators related to the incident, actions taken by all incident handlers, comments, and next steps to be taken.

Documents to be Submitted:

- CIO-SEC-PLN-05 Incident Response Plan

Status and Timeline for Completion: April 2024

5. **OIG recommends that the Peace Corps consistently improve and implement its inventory management process to ensure information system, hardware, and software inventories are accurate, complete, and up-to-date.**

Concur

Response:
The Peace Corps recognizes that to fully understand its information security risk, it must maintain an accurate, complete, and up-to-date inventory of its information systems, hardware, and software. In FY23, the Peace Corps improved and documented its processes that support the tracking of these assets from acquisition to disposal. In late FY23, OCIO implemented tools to improve management of inventory while in service. In FY24, OCIO will continue to update its configuration management processes to codify procedural improvements and the application of these tools for managing inventory.

Documents to be Submitted:

- Asset Management SOP
- CIO-SEC-PLN-02 Configuration Management Plan
- CIO-SEC-PLN-06 Vulnerability Management Plan
- Admin/User Guides for new tools

Status and Timeline for Completion: September 2024

6. **OIG recommends that the Peace Corps improve its vulnerability and patch management processes by consistent and timely remediation of critical and high vulnerabilities as well as patching.**

Concur

Response:
The Peace Corps recognizes the requirement to remediate vulnerabilities in accordance with the organization's assessment of risk and risk appetite. As noted in the findings, the agency is continuing to improve both the technology and processes that support its configuration management program. In the upcoming year, OCIO intends to continue refining and automating its procedures to accomplish consistent, repeatable execution.

Documents to be Submitted:

- CIO-SEC-PLN-06, v8.0, Information Technology Security Program Vulnerability Management Plan

Status and Timeline for Completion: December 2024

7. OIG recommends that the Peace Corps complete and fully implement an identity credential and access management program.

Concur

Response:
The Peace Corps currently has efforts underway to fully implement its Identity Credential and Access Management program. That effort involves fully updating and defining the supporting policies and procedures in addition to ensuring that all staff, both foreign and domestic, are required to employ multi-factor authentication when accessing the Peace Corps' information systems.

Documents to be Submitted:

- MS 542 Information Security Program
- MS 403 Personnel Security Program
- CIO-SEC-PRC-09 Access Controls Guide
- Technical Standard Operating Procedure

Status and Timeline for Completion: April 2024

APPENDIX F: OIG RESPONSE

OIG is encouraged that the agency has concurred with all our recommendations this year. Establishing a strong foundation and culture that integrates information security into business operations, will help ensure that sensitive data is adequately protected.

We also want to stress the importance of dedicating the appropriate resources to carry out this initiative. It is critical that corrective actions are well thought out and applied in a manner that assures the agency can make a sustainable improvement and does not put the Peace Corps' data at risk.