Office of Inspector General

Office
202.692.2900
Website
OIG Reports

Hotline
202.692.2915 | 800.233.5874
Online Contact Form
OIG@peacecorpsoig.gov

To: Carol Spahn, Chief Executive Officer
Thomas Peng, Deputy Chief Executive Officer
Mike Terry, Acting Chief Information Officer
Emily Haimowitz, Chief Compliance Officer

From: Joaquin Ferrao, Acting Inspector General Joaquin Ferrao

Date: September 30, 2022

Subject: Review of the Peace Corps' Information Security Program for FY 2022

Please find attached the annual Report on the Peace Corps' Information Security Program. The Federal Information Security Modernization Act of 2014 (FISMA) requires the Inspector General of each agency to annually conduct an independent assessment of the agency's information security program. We contracted with accounting and management consulting firm Williams, Adley & Company LLP-DC (Williams Adley) to conduct this review.

Williams Adley followed the guidance and instructions provided in OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, and conducted an assessment of the Peace Corps' information security program, including testing the effectiveness of security controls for a subset of systems. The results of the FY 2022 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 rating.

We continue to encourage the agency to dedicate substantial resources for implementing and maturing their information security program. Specifically, we are recommending that the agency (1) establish a comprehensive enterprise risk management program, and (2) develop a strategy and structure that integrates information security into the agency's business operations to strengthen the information security program. Adopting these actions will foster a sustainable culture that incorporates information security across its business operations.

In connection with the contract, we monitored the work performed by Williams Adley. Our monitoring disclosed no instances where Williams Adley did not comply in all material respects with the required sections of U.S. Generally Accepted Government Auditing Standards. Williams Adley is responsible for the attached report dated September 30, 2022, and the conclusions and the overall message expressed therein.

If you or a member of the Peace Corps staff have any questions about Williams Adley's review or our oversight of their review, please contact Assistant Inspector General for Audit Judy Leonhardt at 202-692-2914.

cc: Jackie Dinneen, Acting Chief of Staff
Helen Walker, Chief Information Security Officer
Carl Sosebee, Acting General Counsel
Greg Yeich, Compliance Officer

Peace Corps Office of
INSPECTOR GENERAL

Final Report
Review of the Peace Corps' Information Security Program

September 2022

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, chief information security officers, 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 (FY) 2022.[1]

RESULTS IN BRIEF

The results of the FY 2022 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 rating. In FY 2022, the agency made progress in formalizing several core policies and procedures, such as an Information Security Continuous Monitoring and Supply Chain Risk Management strategies.

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.

We continue to encourage the agency to dedicate substantial resources for implementing and maturing their information security program. Specifically, we assert that focusing on the following two recommendations will elevate their information security program:

- Establishing a comprehensive enterprise risk management program, and
- Developing a strategy and structure that integrates information security into the agency's business operations.

Adopting these actions will foster a sustainable culture that incorporates information security across its business operations. Once the agency integrates information security across all of its business operations the Peace Corps will be able to better identify its information security and organization-wide risks in order to assess and respond to those risks in a timely manner. This, in

[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.

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.

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 information technology (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, three regional recruiting offices, 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 Federal Information Security Modernization Act of 2014 (FISMA),[2] 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, chief information officers, chief information security officers, 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.[3] OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

[2] Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).

[3] E.g., OMB Memorandum M-20-04, Nov.2019.

CHANGES TO THE REPORTING METRICS FOR FY 2022

For FY 2022[4], 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 would 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 (EO) 14028, "Improving the Nation's Cybersecurity," as well as other recent OMB guidance to agencies on the continued efforts to modernization Federal cybersecurity programs.

Further, OMB also adjusted the timeline for the IG's review of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the evaluation of agency effectiveness by the IG finished in October. This timing limited agency leadership's ability to request resources in the next budget year submissions to provide for remediations. For FY 2022, and future years, the results of the IG review are due in July to reduce the time between issue identification, resource request, and allocation.

NIST CYBERSECURITY FRAMEWORK

The IG core 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.
- **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.

[4] OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements

- **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 2022.[5] For more information on the methodology used, see Appendix A. For a list of Federal requirements used as criteria, see Appendix D.

[5] 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

OVERVIEW

The results of the FY 2022 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 rating. In FY 2022, the agency made progress in formalizing several core policies and procedures, such as an Information Security Continuous Monitoring and Supply Chain Risk Management strategies.

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.

We continue to encourage the agency to dedicate substantial resources for implementing and maturing their information security program. Specifically, we assert that focusing on the following two recommendations will elevate their information security program:

- Establishing a comprehensive Enterprise Risk Management (ERM) program, and
- Developing a strategy and structure that integrates information security into the agency's business operations.

Adopting these actions will foster a sustainable culture that incorporates information security[6] across its business operations. Once the agency integrates information security across all of its business operations, the Peace Corps will be able to better identify its information security and organization-wide risks in order to 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.

ENTERPRISE RISK MANAGEMENT

Mandated for the Federal government by the OMB,[7] ERM is an effective tool for strong governance. ERM allows management to understand an organization's portfolio of high-risk exposures, which could affect the organization's success in meeting its mission. As such, ERM is a decision-making tool that allows leadership to view risks from across an organization's portfolio of responsibilities. ERM recognizes how risks interact (i.e., how one risk can magnify or offset another risk), and also examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance. For example, treatment of one risk in one part of the organization can create a new risk elsewhere or can affect the effectiveness of the risk treatment applied to another risk.

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

[7] OMB M 16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.

ERM is part of overall organizational governance and accountability functions and encompasses all areas where an organization is exposed to risk (cyber, financial, operational, reporting, compliance, governance, human capital, reputation, etc.). An effective ERM helps organizations implement strategies to ensure effective use of resources, enable an optimized approach to the identification and remediation of compliance issues, and promote reliable reporting and monitoring across business units.

To implement an ERM program, it is management's responsibility to:

- Identify and understand the core risks facing an organization,
- Determine how best to address those risks, and
- Ensure that the necessary actions are taken.

In support of building ERM, there are two crucial concepts to consider: (a) risk appetite and (b) risk tolerance. OMB defines[8] these concepts as:

> Risk appetite "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior-level leadership (enterprise) and serves as the guidepost to set strategy and select objectives."
>
> Risk tolerance "is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite."

Senior management provides risk guidance through these risk appetite and risk tolerance statements. The organization then manages and monitors processes that balance the risks and resource allocation to demonstrate where risk tolerances have been exceeded or validate that the organization is operating within the defined appetite. The ERM processes should aid the senior management by providing them with a portfolio view of key risks across the organization via risk registers.

OMB Circular A-123 requires that enterprise risks be recorded in a risk register of appropriate content and format. The enterprise risk register is comprised of discipline-specific risks (e.g., cybersecurity, legal, financial), so cybersecurity risks need to be documented and tracked in cybersecurity risk registers in order to support better management of cybersecurity risks at the enterprise level.

CYBERSECURITY INTEGRATION WITH ERM

Cybersecurity risks are risks that could expose the agency to exploitation of vulnerabilities which would 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

[8] OMB M 16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.

enterprises and their component organizations to better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.[9]

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 aggregated, normalized, and prioritized. 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.

ERM AT THE PEACE CORPS

The Peace Corps has struggled to implement a comprehensive ERM program over the years. Despite outlining organizational risk management as one of the agency's key management objectives in their strategic plan starting with FY 2018, the Peace Corps has not yet implemented an ERM program.

Over the last year, the agency has been focusing on completing office level risk registers. As of June 2022, five offices (including the OCIO) had completed risk registers and an additional five offices were in the process of completing their registers. Once these office level risk registers are completed and reviewed, the Peace Corps plans to develop their enterprise level risk register. However, it is still unclear how these office level risk registers will be utilized in developing the enterprise level program. It is also unclear how cybersecurity risks have been incorporated into the office level risk registers and therefore how it will be incorporated into the enterprise level 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. However, these policies and procedures have not defined the agency's risk appetite or risk tolerance, which serves as a fundamental issue in pursuing an effective information security program. The agency has acknowledged that these documents do not reflect the agency's maturing approach to ERM and has plans to update its existing ERM policies and procedures to better align with their program.

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

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. While the Council has been convening more frequently in FY 2022, these meetings are still on an ad-hoc basis, and the group has not yet guided the Peace Corps in its implementation of a more comprehensive risk-based decision-making process.

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. Until recently, the establishment and implementation of ERM has been handled by a variety of staff members as collateral and part-time duties. In May 2022, the agency assigned a full-time resource to assist with the implementation of ERM. Then in July 2022, as part of the FY 2023 budget and strategic investments, a permanent and full-time Chief Risk Officer position was created to oversee and manage the ERM program. Additionally, the existing ERM Council Charter does not include the participation of the Chief Information Security Officer (CISO), an advocate for cybersecurity. Such exclusion of the CISO role further widens the gap between linking cybersecurity risk management and ERM.

CISO Role at The Peace Corps

The head of each agency has a legislative mandate to maintain and improve the security of their agency's information and information systems. In most cases, the agency's internal policies delegate management of the agency's information security to the Chief Information Officer (CIO). Under FISMA, the CIO may then delegate tasks related to information security to the senior agency information security officer (often referred to as CISO).

At the Peace Corps, the CISO role is responsible for establishing, documenting, and implementing an agency-wide information security program, including the development of policies, procedures, and control techniques, to address all applicable requirements for protecting Peace Corps information and information systems.

However, this role has been subservient to the CIO, resulting in a limitation of the senior management's knowledge of the risks facing the organization. This has manifested in the OCIO repeatedly circumventing the security assessment and authorization process, as previously reported by the Office of Inspector General (OIG),[10] allowing multiple information systems to be operational without completing critical steps in the system authorization process:

- In FY 2016, Peace Corps Medical Electronic Documentation & Inventory Control System, which stores highly sensitive Volunteer personal health information, did not go through the appropriate security assessment and authorization process before being brought into production.
- In FY 2017, the agency developed and implemented an online tool for Volunteers to request medication without involving the OCIO or following the assessment and authorization process.
- In FY 2019 and 2020, the agency failed to follow the correct steps when bringing the data center into production.

[10] Review of the Peace Corps' Information Security Program for FY 2021, issued October 31, 2021.

- In FY 2021 and 2022, the backbone of the agency's IT infrastructure operated without undergoing a full and comprehensive system security review to ensure that all proper controls are in place.

For the last 8 years, OIG has reported how the agency continuously struggled to address recurring issues with, but not limited to:

- Incomplete view of its IT environment due to lack of an up-to-date, accurate, and complete inventory of its information systems, including hardware and software assets.
- Inconsistent implementation of vulnerability management.
- Lack of an established identity credential and access management program.

In addition, the Peace Corps has suffered from high turnover and long-standing vacancies in the CISO position. Most recently, the role was vacant for most of FY 2021 and over half of FY 2022. During this timeframe, the Deputy CIO stepped in to be acting CISO; however, this left them to balance between managing business operation concerns and information security matters. Creating a separate CISO office would ensure that senior leadership has continued access to unfiltered information about concerns related to, and the importance of, information security. Such communications are critical to agency's overall risk posture, particularly in the absence of a fully implemented ERM program and historical issues with the agency's prioritization of programmatic and operational needs over information security.

BENEFITS TO AGENCY

By focusing on ERM and elevating the role of the CISO, the agency will foster a culture that fully integrates information security into its business operations. This will allow 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 able to achieve an effective information security program.

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.

By empowering the CISO with their own independent office, the agency can ensure cybersecurity risks, which flow as an undercurrent in all business operations, are appropriately identified and elevated to senior management in a timely manner. Thus, allowing these global risks to be better defined and preventing unmitigated vulnerabilities from resulting in financial, reputation, and mission impacts. For example, a cybersecurity event can have consequences that compromise the integrity of financial statements (e.g., income statement, balance sheet, cash flow), or expose sensitive Volunteer information, such as sexual assault and health information to the public or a nefarious organization. Furthermore, a cybersecurity event could lead to downtime within a business unit and prevent the agency from achieving its strategic objectives.

In addition, elevating the CISO role in conjunction with fully implementing an ERM program, will streamline senior leadership focus and prioritize attention based on risk. By developing and implementing a formalized, and systematic approach to evaluate risk, the agency can better automate this process and ensure uniformity in how issues are evaluated and prioritized. Considering cybersecurity risks in light of the agency objectives enables a proactive and mission-oriented view and supports decisions by senior leadership.

LIST OF RECOMMENDATIONS

1. OIG recommends that the Director develop 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. OIG recommends that the Director appoint the chief information security officer to serve on the Enterprise Risk Management Council as a voting member.

3. OIG recommends that the Director further define and implement the Enterprise Risk Management program to ensure information security risks are communicated and monitored at the system, business process, and entity levels.

4. OIG recommends that the Chief Information Officer perform a full security assessment of the General Support System to obtain a complete understanding of system weaknesses.

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

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 2022 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 2022:

- Peace Corps General Support System (PCGSS)
- PC Medical Electronic Documentation & Inventory Control System (PCMEDICS)
- Global Operations (GOPS)

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 2022. 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, 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 Chief Information Officer Metrics (FY 2022)
- 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-22-05 "Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements"
- NIST Special Publications 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

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
GOPS	Global Operations
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

APPENDIX D: GUIDANCE

The following National Institute of Standards and Technology (NIST) guidance and Federal standards were used to evaluate the Peace Corps' information security program.

I. Identify

a. Risk Management

i. NIST Special Publication (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 (ERM)

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 2022 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 Special Publication (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 RESPONSE TO THE PRELIMINARY REPORT

Peace Corps

MEMORANDUM

To: Joaquin Ferrao, Acting Inspector General

EMILY HAIMOWITZ Digitally signed by EMILY HAIMOWITZ Date: 2022.09.13 07:56:00 -04'00'

Through: Emily Haimowitz, Chief Compliance Officer Signature

Peng, Thomas Digitally signed by Peng, Thomas Date: 2022.09.12 23:29:02 -04'00'

From: Thomas Peng, Deputy Chief Executive Officer Signature

Date: September 14, 2022

CC: Carol Spahn, Acting Chief Executive Officer
Jackie Dinneen, Acting Chief of Staff
Lila Jaafar, White House Liaison
Carl Sosebee, Senior Advisor to the Director
Kristin Wells, General Counsel
Michael Terry, Acting Chief Information Officer
Helen Walker, Chief Information Security Officer
Gregory Yeich, Compliance Officer
Judith Leonhardt, AIG/Audits

Subject: Review of the Peace Corps' Information Security Program for FY 2022

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 2021 given to the agency on August 15, 2022.

1. **OIG recommends that the Peace Corps develop 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 is committed to integrating information security into the agency's business operations. In coordination with the development of the agency's Enterprise Risk Management (ERM) program, the agency intends to expand the information security responsibilities across all relevant offices and stakeholder bodies. The long-term goal is for expanded information security responsibilities to be documented in a comprehensive agency information security strategy.
   Initially, the Chief Information Security Officer (CISO) will produce an outline of a project plan for the development of a comprehensive information security strategy. The agency expects that this outline will identify a need for additional resources to be able to develop and implement the information security strategy. The CISO will work to obtain the required additional resources towards this project, which may include staff to develop the detailed project plan for execution.
   The CISO and the Chief Risk Officer will begin having ongoing meetings to ensure the development of the ERM strategy and information security plan are aligned. They will also review office level risk registers to provide the CISO with all of the available current information.
   Document to be Submitted:
   - Outline for comprehensive integration of Information Security Strategy into business operations
   - Documentation regarding additional resources allocated to this initiative
   - Results of ongoing meetings with the Chief Risk Officer and/or other stakeholders

   Status and Timeline for Completion: May 2023

2. **OIG recommends that the Director appoint the chief information security officer to serve on the Enterprise Risk Management Council as a voting member.**

   Concur
   Response: The Peace Corps is in the process of developing its Enterprise Risk Management (ERM) program, in addition to updating the ERM Council charter. The agency has made great progress in furthering this program in Fiscal Year 2022. Some of the progress includes creating and staffing a Chief Risk Officer position, developing office-level risk registers for all major agency offices, ensuring all decision memos are reviewed to identify whether risk-based conversations are needed, and developing and piloting a framework for ad-hoc risk-based ERM Council discussions. The Peace Corps is committed to continuing the progress, which will include holding quarterly ERM Council meetings, creating an agency risk register and risk appetite statement, and

updating the ERM governance documents, including the voting process within the Council, as needed. All of these processes, along with an updated ERM Council Charter when ready, will ensure that information security risks are monitored and brought to the council in an equal manner to all other risks.

Documents to be Submitted:

- Revised Enterprise Risk Management Council Charter
- ERM Council Meeting Minutes

Status and Timeline for Completion: December 2023

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

Concur
Response: The Peace Corps remains committed to the development and operation of its Enterprise Risk Management (ERM) program. Some of the progress made to establish this program is described in response to recommendation two. In addition, the agency has initiated its effort to develop a comprehensive ERM Strategy. All offices and senior leaders, including the CISO, will be involved in this effort.

The Peace Corps intends to finalize the ERM Strategy which articulates the risk philosophy, architecture, governance, and processes that monitor and communicate risk between all levels of the organization. The ERM Strategy will address information security in addition to other significant categories of risk most relevant to the organization and impactful to mission success. This Strategy will include the agency's risk appetite relevant to those risk categories which, in turn, will inform defining risk tolerances of mission supporting services, risk response, and business continuity planning.

Document to be Submitted:

- Peace Corps Enterprise Risk Management Strategy
- Revised Enterprise Risk Management Council Charter
- ERM Council Meeting Minutes

Status and Timeline of Completion: December 2023

4. **OIG recommends that the Chief Information Officer perform a full security assessment of the General Support System to obtain a complete understanding of system weaknesses.**

Concur

Response: The full security assessment of the General Support System (GSS) began in July 2022 and is scheduled to be completed by October 2022. Peace Corps internal policies provides up to 60 days to fix or plan a corrective action strategy after the outcome of a GSS Security Assessment Report. Therefore, by December 2022 the agency will complete its full assessment, including resolving any issues or developing its corrective action plan.

Documents to be Submitted:

- GSS Security Assessment Report
- Plans of Action and Milestones

Status and Timeline of Completion: December 2022

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 Fiscal Year (FY) 2022, the Peace Corps improved and documented its processes that support the tracking of these assets from acquisition to disposal. In late FY22, the agency invested in tools intended to improve management of that inventory while in service. In early FY23, OCIO will 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: February 2023

APPENDIX F: OIG COMMENTS

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.

Making a culture shift is a large undertaking; therefore, it is critical for the Peace Corps to establish an accountability structure as part of its efforts. Having someone who takes ownership of the program and recognizes the importance of integrating information security into all business decisions will ensure the program's success and longevity.

We also want to stress the importance of dedicating the appropriate resources to carrying 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.