Office of Inspector General

Office
202.692.2900
Website
OIG Reports

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

To: Carol Spahn, Acting Director
Dave Noble, Chief of Staff
Thomas Peng, Chief Information Officer
Emily Haimowitz, Chief Compliance Officer

From: Kathy A. Buller, Inspector General

Date: October 29, 2021

Subject: Review of the Peace Corps' Information Security Program for FY 2021

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-21-02, *Fiscal Year 2020-2021 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 this assessment placed the Peace Corps at Level 2, Defined, which is an improvement over prior years where the agency was only able to achieve Level 1, Ad-hoc. While policies and procedures have been developed, systemic weakness in the Peace Corps' information security program continue to exist because the agency has not fully adopted the risk-based approach to improve its IT security posture. Specifically, the agency lacks (1) an understanding of their operating environment, (2) a comprehensive risk management strategy, and (3) an independent information security office. The report makes four recommendations that, if effectively implemented, should help elevate and strengthen the Peace Corps' information security program.

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 October 29, 2021, 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, Deputy Chief of Staff
Lila Jaafar, White House Liaison
Michael Terry, Deputy Chief Information Officer

Carl Sosebee, Senior Advisor to the Director
Kristin Wells, General Counsel
Colin Jones, Compliance Officer

Peace Corps Office of
INSPECTOR GENERAL

Final Report
Review of the Peace Corps' Information Security Program

October 2021

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) 2021.[1]

RESULTS IN BRIEF

The results of the FY 2021 review, which assessed the agency's performance against a government-wide maturity model, placed the Peace Corps at Level 2, Defined, which is an improvement over prior years where the agency was only able to achieve Level 1, Ad-hoc. Since our last review, the Peace Corps has made progress in formalizing several core policies and procedures, such as an Information Security Continuous Monitoring strategy.

Despite documenting policies on paper, the Peace Corps Office of Inspector General (OIG) remains concerned about the quality of the agency's information security program since the agency's actions demonstrate that the Peace Corps has not fully adopted a risk-based approach and incorporated information security into its business decision-making process. This is consistent with more than a decade of OIG reviews outlining apprehensions over the agency's management of information security, especially considering the sensitive data that the Peace Corps maintains, notably employee personnel records, Volunteer health records, and Volunteer sexual assault incident information.

The most significant finding from this year's review relates to the Peace Corps' ongoing disregard for the importance of the General Support System (GSS) assessment and authorization process. As a recurring issue from prior years, the Peace Corps' GSS – which serves as the backbone of the agency's IT infrastructure – still operates without undergoing a full and comprehensive system security review to ensure that all proper controls are in place. This particular instance is illustrative of a larger systemic weakness in the Peace Corps' information security program, where even though policies and procedures are defined, the agency has not fully adopted the risk-based approach to improve its IT security posture. Specifically, the agency

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

lacks (1) an understanding of their operating environment, (2) a comprehensive risk management strategy, and (3) an independent information security office.

The consequence of a fragile information security program can be catastrophic. Without a clear understanding of its security environment and an organization-wide view of risks, the Peace Corps is not able to identify, assess, and respond to those risks in a timely manner, which in turn, exposes the agency to targeted attacks and environmental disruptions. This also gives rise to inefficient use of resources as efforts are spent in a reactive manner to address issues as they surface, instead of proactively preventing and addressing the weaknesses.

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: to help people of interested countries in meeting their need for trained Volunteers; to help promote a better understanding of Americans on the part of the peoples served; and 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, 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 information 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.

NIST CYBERSECURITY FRAMEWORK

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued in February 2013, requires the creation of a risk-based cybersecurity framework that outlines a set of industry standards and best practices to help agencies manage their cybersecurity or information security risks. NIST developed the resulting framework through collaboration between government and private sector entities. The Cybersecurity Framework can be used to help identify risk and align policy and business approaches to manage that risk. The Cybersecurity Framework outlines five function areas that direct the efforts to improve information security risk management:

- **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

The FY 2021 IG FISMA Metrics provide maturity models for all five security functions aligning with the Cybersecurity Framework. This helps to promote consistent and comparable metrics and criteria in the IG review process while providing agencies with a meaningful independent assessment of the effectiveness of their information security programs on a five-level scale:

- **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. Generally, 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 2021.[4] For more information on the methodology used, see Appendix A. For a list of Federal requirements used as criteria, see Appendix D.

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

RESULTS

OVERVIEW

The results of the FY 2021 review, which assessed the agency's performance against a government-wide maturity model, placed the Peace Corps at Level 2, Defined, which is an improvement over prior years where the agency was only able to achieve Level 1, Ad-hoc. Since our last review, the Peace Corps has made progress in formalizing several core policies and procedures, such as an Information Security Continuous Monitoring strategy. However, the policies developed do not cover all of the required aspects of information security; therefore, the agency will need to continue to dedicate substantial resources and energy to maturing their information security program.

Furthermore, despite documenting policies on paper, the agency's actions demonstrate that the Peace Corps has not fully adopted a risk-based approach and incorporated information security into its business decision-making process. Since FY 2019, Williams Adley has reported that the agency has failed to ensure the backbone of its IT infrastructure, known as the GSS, is secure. The GSS continues to operate without undergoing a full and comprehensive system security assessment to ensure that all proper controls are in place. Without this complete assessment, the Peace Corps continues to put the agency's sensitive data and information systems at risk.

Furthermore, by continually improperly reviewing and failing to complete a full and comprehensive system security assessment on the GSS, the agency has wasted time and resources. Each independent assessment takes months of preparation, review, and reporting. Re-assessing the GSS multiple times has required excessive time and resources not only for this project, but it has also diverted efforts away from assessing other critical Peace Corps systems, including the agency's financial system.

A shift towards more information security-focused mindset requires serious and sustained undertaking with involvement and dedication from every level of the organization, especially at the executive levels. However, one of the crucial roles in emphasizing and voicing the importance of information security, Chief Information Security Officer (CISO), was left vacant for a majority of FY 2021. The agency does not have the appropriate structure in place to promote effective planning, resources, and communications necessary to achieve an effective information security program. Further, despite similar reports in the past, the agency has not put in place measures that would suggest a sense of urgency in addressing this challenge.

FAILED ASSESSMENT AND AUTHORIZATION PROCESS

All information systems should undergo an assessment of their information security controls to ensure effectiveness. This process includes identifying information security risks to the system and designing controls to mitigate these risks and adequately protect the information within the system. The agency must document these controls in a system security plan and have these controls tested by an independent assessment team. Upon completion of this independent assessment, information security weaknesses identified are either remediated immediately or a remediation plan is developed with estimated completion dates. The agency's Authorizing Official then reviews the assessment results and remediation efforts to determine whether to formally authorize the operation of that system and accept the risks this system poses to the organization if operational. Upon approval, the system receives an Authority to Operate (ATO).

History of the Failed GSS Assessments

In FY 2019, the Peace Corps undertook the largest change to the agency's IT infrastructure in over seven years by moving the headquarters portion of the GSS offsite to a commercial data center (referred to as "the data center" in this report). However, in making this change, the agency failed to follow its own assessment and authorization process to ensure there were adequate security controls in place. The data center underwent two independent assessments; the first assessment resulted in the system failing 100 percent of the 135 security controls reviewed. The second assessment, which occurred 6 weeks later, resulted in the system failing over 50 percent of the 91 security controls reviewed.[5] After the second assessment, the data center received a one-year ATO, which was contingent on the maintenance and management of the security posture of the system. In FY 2020, Williams Adley determined that the Peace Corps did not fulfill these requirements and therefore, invalidated the ATO.

In FY 2020, the Peace Corps changed the make-up of the GSS, adding back the data center with components that supported over 60 different locations, the new headquarters building, all overseas posts, and three domestic recruiting offices.[6] The agency pursued an assessment of this new GSS in October 2020. However, the results of this assessment were less than favorable. The independent assessment report stated that the agency:

> did not perform due diligence in preparing, reviewing, and documenting the System Security Plan Package of documentation as required by the Risk Management Framework, security control implementation artifacts, and Peace Corps Policy to develop and manage a complete suite of security documents for the system.

The independent assessment also determined that there were control weaknesses in 88 percent of the 234 security controls. As part of the independent assessment, vulnerability scans of different system components are to be evaluated; however, the agency was not able to provide scans that accounted for all the GSS components. Equally concerning is that of the scans provided, there were over 16,000 critical and high vulnerabilities identified. The assessment ranked the overall risk for continued operations of the GSS as high and recommended that the agency grant a nine-month ATO, revise its documentation, and conduct a reassessment of the GSS. In November 2020, the GSS received a nine-month ATO. OIG believed that this was the agency's opportunity to diligently rebuild the GSS information security control foundation and undergo the proper security assessment and authorization process.

However, in FY 2021, the Peace Corps did not pursue a new comprehensive independent assessment of the GSS. Instead, in September 2021, the agency completed a partial independent assessment of 77 controls, or one third of the GSS's security controls. This assessment resulted in control weaknesses being identified in 57 percent of the 77 controls reviewed. Many of these weaknesses highlighted deficiencies within the system security plan where controls were not sufficiently described. Furthermore, while the independent assessment team attempted to obtain vulnerability scans for the GSS components, the agency did not provide any to the assessors. The GSS has not received an ATO from this FY 2021 assessment yet. However, the system was granted a three-month extension to the existing ATO on August 5, 2021 with contingencies on prioritizing the mitigation of specific weaknesses.

[5] Review of the Peace Corps' Information Security Program for FY 2019, issued October 31, 2019.

[6] Review of the Peace Corps' Information Security Program for FY 2020, issued October 31, 2020.

Ensuring all proper controls of the GSS are adequately developed and implemented is essential as it supports all business functions. The failure to pursue a comprehensive assessment and authorization process puts all Peace Corps information systems and sensitive data at serious risk.

Cascading Impacts to Other Peace Corps Systems
With the GSS still undergoing assessment in FY 2021, other systems that rely on the GSS full ATO are currently pending their own assessment and authorizations. For example:

- The Volunteer Delivery System's system security plan was not updated and finalized, and a security control assessment was not conducted in FY 2021.
- The Financial System security control assessment was not conducted in FY 2021.

As the GSS is the backbone of the Peace Corps' IT infrastructure, it provides connectivity, security, storage, and data access for its employees and contractors. Many systems within the Peace Corps infrastructure rely on the GSS for inherited controls. Negligence in the GSS's security posture review can leave other critical systems, including the financial system, vulnerable to known, and potentially unknown, common and critical information security risks.

Unresolved Plan of Actions and Milestones
The Plan of Action and Milestones (POA&Ms) process is a method to address and manage information security weaknesses within the Peace Corps environment, including the information security control failures identified from the independent control assessment. These POA&Ms track the needed tasks to be accomplished, the resources required, any milestones, and estimated completion dates to resolve the information security weakness. However, we determined that the Peace Corps did not document and track all required attributes for certain weaknesses within the POA&M listing. As of October 2021, there are weaknesses from 2019 to be remediated and are currently marked as delayed within the POA&M listing. Furthermore, weaknesses identified from the previous GSS assessments have also been delayed, resulting in half of the POA&Ms overdue on their estimated completion dates. The POA&M process is critical in ensuring the information security infrastructure remains effective.

REASONS FOR AN INEFFECTIVE INFORMATION SECURITY PROGRAM

While the Peace Corps has been able to make some advancements in their information security program, the agency does not have the people, processes, or technology in place to achieve an effective information security program that meets the government standard of Level 4, Managed and Measurable. Level 4 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. Specifically, the agency lacks:

- An understanding of their operating environment.
- A comprehensive risk management strategy.
- An independent information security office.

Defining the IT Environment

In order to understand information security risk, an organization must first clearly identify its environment, including what hardware and software assets it owns and how these assets interconnect with each other. Understanding where the agency's system boundaries lie is critical to knowing how to protect the information residing within the Peace Corps network.

Over the years, the Peace Corps has continued to struggle to have a full and clear visibility of its IT environment. Even though there are some defined processes to manage system inventory, the agency does not truly have an up-to-date, accurate, and complete inventory of its information systems, including hardware and software assets.

For the October 2020 independent assessment, the agency was not able to provide vulnerability scans that matched the inventory as described in the GSS system security plan. Specifically, vulnerability scans could only be provided for 34.4 percent of listed components. Additionally, the report noted that scans were not being performed on all types of components within the boundary. In the GSS assessment conducted this year, the Peace Corps was not able to provide any vulnerability scan results to demonstrate its clear understanding of how data is stored and where data flows within its GSS system to independent assessor.

However, subsequent to the assessment, the agency was able to gather applicable vulnerability scan results for the Authorizing Official's review. However, when asked, the agency could not confirm whether these scans represented the full inventory of components within the GSS boundary.

This suggests the agency lacks foundational knowledge and sufficient planning in understanding what is truly within its IT environment, and how each asset can expose the agency to significant risks. Without knowing what is within the system boundaries, the Peace Corps is not aware of the weaknesses that may exist, and in turn, fails to remediate the vulnerability and protect the assets adequately.

In an attempt to gain a broader understanding of its IT system, the Peace Corps developed an Enterprise Architecture in April 2021. An Enterprise Architecture provides a high-level blueprint of the information and operation technologies within an agency's environment. Establishing an Enterprise Architecture offers agencies greater visibility and understanding of its systems and how they are connected to one another, while outlining security controls to increase protection of the systems. However, the agency's approach to an Enterprise Architecture only includes security architecture from a governance standpoint.

Specifically, it does not highlight how particular security controls or practices tie to the agency's strategic goals and objectives. Moreover, without an extensive knowledge of all its systems and assets, the Peace Corps has no assurance that the security requirements are consistently met and in alignment with the risk management strategy.

Insufficient Enterprise Risk Management Program

To emphasize the importance of protecting critical infrastructure, Executive Order 13800[7] was issued in 2017 to hold agency heads accountable for managing cybersecurity or information security risk in their organizations. Specifically, Executive Order 13800 defines effective risk

[7] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

management as requiring agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources. Furthermore, Executive Order 13800 requires agency heads to use the Cybersecurity Framework to manage the agency's cybersecurity risk and hold agency heads accountable for ensuring that cybersecurity or information security risk management processes are aligned with strategic, operational, and budgetary planning processes.

The Peace Corps has outlined organizational risk management as one of the key management objectives since 2018; however, appropriate resources have not been dedicated to the program. In July 2019, the agency established the Enterprise Risk Management (ERM) Council with the responsibility of reviewing, evaluating, and monitoring opportunities and risks to the agency's ability to achieve its mission and strategic objectives. The ERM Council is one part of the agency's efforts to implement an ERM program. However, the council is still in the early stages and has not yet guided the Peace Corps in its' implementation of a more comprehensive risk-based decision-making process. In addition, the agency has created internal risk registers for two of the agency's offices (including the OCIO) and presented them to high-level executives. However, it is not clear whether any value was derived from this exercise since the ERM Council did not meet in FY 2021.

Empowering the Chief Information Security Officer

Information security needs a voice within senior management, someone to provide 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.

The CISO position was vacant for the majority of FY 2021. The lack of an independent voice within OCIO created a void to advocate for security focused decisions and left the Deputy Chief Information Officer to balance between managing business operation concerns and security matters. The agency historically has prioritized programmatic and operational needs to the detriment of information security as the OIG has previously reported.

In FY 2020, we recommended that the Peace Corps Director designate the CISO position and team members to a new office that is independent from the Chief Information Officer (CIO), with these two separate offices reporting to the same senior executive. We believe the creation of an independent office will provide the CISO more autonomy in making and executing information security risk-based decisions on behalf of the agency, while allowing the CIO to focus more on strategic IT goals and departmental leadership. Unfortunately, this recommendation was rejected by the agency.

Response to FY 2020 recommendation to elevate the CISO position:

> Peace Corps is interpreting the chief information security officer (CISO) position authority as defined in FISMA Law 2014 in that the agency head is responsible for IT Security and delegates those duties to CIO to ensure compliance. The CIO then designates the CISO to carry out the IT Security responsibilities. In addition to following FISMA 2014, many other small Federal agencies have the CISO report to the CIO so the agency will continue with that reporting structure. The CISO will continue to meet monthly with the Director, and retain membership on the Enterprise Risk Management Secretariat, Senior Policy Committee, and the Technology Advisory Board.

As outlined in the agency's response to our recommendation, while the law allows the agency head to delegate the duties to ensure compliance with information security requirements to whomever they seem fit, more than a decade of OIG reports supports our finding and recommendation. During the last eight years, OIG has repeatedly reported how the agency has continuously neglected to consider information security when making business decisions. Specifically, the OCIO has repeatedly circumvented the security assessment and authorization process allowing multiple information systems, to be operational without completing critical steps in the 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.

IMPACT TO THE AGENCY

Per NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View, organizations in the public and private sectors depend on technology-intensive information systems to successfully carry out their missions and business functions. Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

Without a clear understanding of its information security environment and an organization-wide view of risks, the Peace Corps is not able to identify, assess, and respond to those risks in a timely manner, which in turns, exposes the agency to targeted attacks and environmental disruptions. This also gives rise to the inefficient use of resources as efforts are spent in a reactive manner to address issues as they surface, instead of proactively preventing and addressing the weaknesses. In addition, the lack of proper tone-at-the-top leadership and increased attention to information security discourages the Peace Corps from achieving an effective information security program.

The consequence of a weak information security program can be catastrophic. In the Federal government, the Office of Personnel Management (OPM) faced a major compromise to its network and sensitive information in 2014. The cause of the attack was attributed to poor information security, including missing two-factor authentication, lack of understanding the complete IT environment, no defined standards for hardware and software, out of date system authorizations, and poor patching. As the Peace Corps environment carries similar IT security weaknesses to those that led to the OPM breach, the agency has not adequately integrated IT security with business operations to ensure the protection of our operations, reputation, and ability to keep Volunteers safe.

RECOMMENDATIONS

1. OIG recommends that the Director move the chief information security officer position and staff to a new office that is independent from the chief information officer. These two separate offices should both report to the same senior executive.

2. 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.

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

4. 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.

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 2021 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 testing the effectiveness of security controls for a subset of systems as required, for FY 2021:

- Peace Corps General Support System (PCGSS)
- Peace Corps Volunteer Delivery System (VDS)

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 May to October 2021. 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 2021)
- 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-21-02 "Fiscal Year 2020-2021 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

ATO	Authority to Operate
CISO	Chief Information Security Officer
CIO	Chief Information Officer
DHS	U.S. Department of Homeland Security
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GSS	General Support System
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
OPM	Office of Personnel Management
POA&M	Plan of Action and Milestones
SP	Special Publication

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) 800-39, *Managing Information Security Risk: Organization, Mission, and System View*

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 800-53 Revision 4, *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. OMB M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*

vii. DHS Binding Operative and Emergency Directives

viii. Federal Enterprise Architecture Framework (Version 2)

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

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

xi. OMB Circular M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*

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

II. Protect

a. Configuration Management

i. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

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

iii. OMB Circular M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*

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

b. Identity and Access Management

i. NIST SP 800-53 Revision 4, *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. Federal Identity, Credential, and Access Management (FICAM) Implementation Guidelines

iv. FIPS 140-2, *Security Requirements for Cryptographic Modules*

v. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

vi. OMB Circular M-19-17, *Enabling Mission Delivery through Improved Identity Credential, and Access Management*

c. Security and Privacy Training

i. NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*

ii. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*

iii. Federal Cybersecurity Workforce Assessment Act of 2015

d. Data Protection and Privacy

i. NIST SP 800-53 Revision 4, *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 Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*

III. Detect

a. Information Security Continuous Monitoring

i. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

ii. 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

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

iii. 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 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*

ii. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

APPENDIX E: AGENCY RESPONSE TO THE PRELIMINARY REPORT

Peace Corps

MEMORANDUM

To: Kathy Buller, Inspector General

Through: Emily Haimowitz, Chief Compliance Officer

Haimowitz, Emily Digitally signed by Haimowitz, Emily Date: 2021.10.25 14:30:06 -04'00'

From: Thomas Peng, Chief Information Officer

Peng, Thomas Digitally signed by Peng, Thomas Date: 2021.10.25 14:37:59 -04'00'

Date: October 25, 2021

CC: Carol Spahn, Acting Director
Dave Noble, Chief of Staff
Lila Jaafar, Deputy Chief of Staff/White House Liaison
Carl Sosebee, Senior Advisor to the Director
Kristin Wells, General Counsel
Michael Terry, Deputy Chief Information Officer
Colin Jones, Compliance Officer
Joaquin Ferrao, Deputy Inspector General
Judith Leonhardt, AIG/Audits

Subject: Review of the Peace Corps' Information Security Program for FY 2021

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 October 15, 2021.

Cybersecurity has often been viewed as a barrier to modernization and technical progress, resulting in the implementation of information systems with little regard for securing or safeguarding them. In 2017, the Agency prioritized information security and risk management to reshape this culture across the organization. Since that time, numerous changes have been made to information security policies, processes, tools and culture in order to grow and strengthen its security and risk management programs. Going forward, the agency will continue to focus on rigorous implementation and continuous enhancements of those programs.

1. OIG recommends that the Director move the chief information security officer position and staff to a new office that is independent from the chief information officer. These two separate offices should both report to the same senior executive.

Do Not Concur
Response: The OIG recommendation is premised on past failures of the CIO to prioritize IT security and engage with agency leadership in evaluating and mitigating IT security related risks. The Federal Information Security Modernization Act of 2014 (FISMA) directs agency heads to delegate authority to ensure compliance with the law to agency chief information officers (CIO), who in turn are required to designate a senior agency information security officer to carry out the CIO's responsibilities (see 44 U.S.C. § 3554(a)(3)). These IT security officials are generally referred to as chief information security officers (CISO).

In recent years, however, agency leadership and the CIO have prioritized IT security in both word and deed. Peace Corps' CIO and CISO actions include revision of agency policies and policy development to help lead IT security transformation efforts and compliance, prioritization of security related investments by restructuring IT's budget to put more resources into the cybersecurity budget to help develop organizational change efforts, and the establishment of an Enterprise Risk Management (ERM) program that supports development of a cohesive cybersecurity architecture and plan that will provide a more robust digital maturity model for the agency's ERM program.

The CISO has been added to the Technical Advisory Board, Enterprise Risk Management Council, and the Policy Secretariat as an Advisor to the Senior Policy Committee. The CISO, CIO and System Owners have met every two weeks since early this year to discuss IT risks across the agency portfolio as partners to ensure that OCIO protects the privacy of personally identifiable information and provides effective strategies to secure the agency's information technology. The CIO, in turn, regularly communicates with senior executives to discuss those risks and deliberate on appropriate responses. In the next few weeks, work will begin on chartering the organization-level Cybersecurity Steering Committee, which will be chaired by the CISO and charged with coordinating agency security planning, operational oversight and reporting. It is the agency's contention that these collective steps meet the intended goal of OIG's recommendation.

Realigning the CISO's office out of the OCIO will introduce unnecessary challenges and inefficiencies.

- The OCIO and a dozen other offices already report to the Chief of Staff. Introducing another office will increase the demands on that executive's time, reducing attention overall.
- Presenting risk apart from operations cultivates the negative perception that the two are in opposition. That perception frames security as a hurdle to be overcome or, worse still, to be worked around. Even within OCIO, dismantling this perception required the embedding of the CISO's staff into the daily operations of information system teams.
- Separating the CISO and CIO into independent offices will diminish visibility into the daily activities of the OCIO. Currently, that visibility drives activity into the security framework that, otherwise, would have been deemed too trivial to include IT Security.

At the 2017 FISMA exit brief, the OIG and Williams-Adley shared that maturing the program would take years to achieve but thought that the program was moving in the right direction. Many of the technical, structural, and cultural changes necessary for a successful and more robust security program have come into fruition in the last four years. While there is still much to do, the agency is now better positioned to strengthen and mature its information security and risk management capabilities.

Documents Submitted:

- Executive-level correspondence on IT security matters
- Biweekly Cybersecurity Working Group minutes
- Draft Cybersecurity Steering Committee charter

Status and Timeline for Completion: N/A

2. 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: Peace Corps concurs with this recommendation. Under the leadership of the CISO, Peace Corps' General Support System will undergo a complete reassessment in order to obtain a complete understanding of its system weaknesses. In addition, the CISO with the support of OCIO, will modify its continuous monitoring strategy to mandate the reassessment of identified control weaknesses, in addition to the one-third of system security controls that are assessed annually. This will help ensure appropriate monitoring and procedures are in place for detecting, reporting, and responding to security incidents, and that contingency plans and procedures for the agency information systems are secure.

Documents to be Submitted:

- Updated CIO-SEC-PLN-01 Continuous Monitoring (ISCM) Strategy
- PCGSS FY22 Security Assessment Report (SAR)

Status and Timeline for Completion: September 2022

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

Concur
Response: Peace Corps will further define and implement its ERM program to ensure information security risks are communicated and monitored at the system, business process, and entity levels. The agency is adding additional resources to fully implement the ERM program, including onboarding two intermittent experts who will be assigned to help establish agency risk tolerances and assist with the development of office risk registers and profiles.

Documents to be Submitted:

- ERM SOP
- Cybersecurity Risk Register
- CIO-SEC-PRC-01 Managing IT Risk
- ERM meeting minutes

Status and Timeline for Completion: May 2022

4. 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: Peace Corps will continue to improve and refine its business processes and tools to identify, record, track, manage and scan its information systems, hardware and software to help regulate the inventory within its operations.

Documents to be Submitted:

- CIO-SEC-PLN-02 Configuration Management Plan
- CIO-SEC-PLN-06 Vulnerability Management Plan

Status and Timeline for Completion: April 2022

APPENDIX F: OIG COMMENTS

OIG regrets the Peace Corps' decision to non-concur with recommendation 1—to have the chief information security officer (CISO) manage an independent office —and urges the agency to reconsider this recommendation and reevaluate this decision. A decade of OIG reports illustrates the need to make fundamental and far-reaching changes to the Peace Corps' approach to cybersecurity. The Peace Corps' implementation, where the CISO's role is subservient to the CIO, has resulted in limiting the senior management's knowledge of the risks facing the organization. Without such awareness, the Peace Corps' enterprise risk-based decision making is hobbled and remains highly susceptible to compromising sensitive data that the Peace Corps maintains, most notably employee personnel records, Volunteer health records, and Volunteer sexual assault incident information.

The agency's response clearly demonstrates why the CISO role needs to be elevated as the agency has a limited, and antiquated way, to view information security. In their response, the agency discusses how elevating the CISO role outside of the Office of the Chief Information Officer (OCIO) will introduce unnecessary challenges and inefficiencies by separating risk analysis from operations and limiting the visibility of OCIO activities. However, information security risks flow as an undercurrent in all business operations and decisions, not just within OCIO. By elevating the CISO, the agency will allow these global risks to be better defined and prevent 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.

Furthermore, the agency states that creating a new office would put undue demands on executives' time and reduce attention. However, elevating the CISO role in conjunction with our recommendation 3, to fully develop the Enterprise Risk Management (ERM) program, will streamline senior leadership focus and prioritize attention based on risk. Currently, the agency evaluates each emerging issue separately and assesses its impacts and risks to the agency on an ad hoc basis. By developing and implementing a formalized, systematic program 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 enterprise objectives, enables a proactive and mission-oriented view and supports decisions by senior leadership.

We also want to emphasize that throughout the agency's response there is discussion regarding how the CISO position has been incorporated into decisions. However, it is important to note that the CISO position is currently vacant, as it was for the majority of FY 2021. This has removed the independent voice from conversations, since the Deputy Chief Information Officer has been acting in the CISO role, while also balancing this role with their operations focused concerns. Unfortunately, the current situation with the CISO position is not an anomaly. The position has been plagued by vacancies and other situations which under the current model has institutionally diminished or crippled the role of the CISO. The CISO position needs to be elevated and distinctively focused on identifying and raising security concerns.

In the response, the agency references OIG comments from FY 2017. OIG was hopeful that the agency would take the opportunity to establish a strong foundation and mature its information security program over the years. However, that has not occurred at the pace necessary to deal with myriad cybersecurity risks. The frequency, creativity, and severity of cybersecurity attacks have increased dramatically. Alarmingly, our reports in the last four years have outlined ineffective security program ratings and repeated egregious deficiencies related to the General Support System and the associated data center which is the backbone of Peace Corps IT system.