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: Jody Olsen, Director
Michelle Brooks, Chief of Staff
Scott Knell, Chief Information Officer
Angela Kissel, Chief Compliance Officer

From: Kathy A. Buller, Inspector General

Date: October 30, 2020

Subject: Review of the Peace Corps' Information Security Program for FY 2020

Please find attached the annual Report on the Peace Corps' Information Security Program. This review was conducted to assess the effectiveness of the security controls and practices. The report makes four recommendations that, if effectively implemented, should help elevate and bring attention to the Peace Corps' information security program, which we in turn hope will strengthen the information security program overall.

We contracted with accounting and management consulting firm Williams, Adley & Company LLP-DC (Williams Adley) to review the Peace Corps' Information Security Program as of September 30, 2020. OMB Memorandum M-20-04 ("Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements") provides instructions for meeting this year's reporting requirements.

The work was performed to meet Government Auditing Standards, GAO-18-568G, (GAGAS), 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. In all other respects, Williams Adley met the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

Williams Adley's report for FY 2020 includes an 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) 2020. In its review of the Peace Corps, Williams Adley assessed the agency's performance against a government wide maturity model, and placed the Peace Corps at Level 1, ad-hoc, or operating in a reactive manner. Specifically, the Peace Corps lacks an effective information security posture. Williams Adley found:

- The backbone of the agency's IT infrastructure operating without undergoing the proper assessment and authorization; and
- Outdated IT assets operating without adequate protections.

The conclusions and the overall message expressed in the attached report dated October 30, 2020, are based on Williams Adley's results of the FISMA evaluation. Also, our review

disclosed no instances where Williams Adley did not comply in all material respects with the required sections of GAGAS.

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: Matthew McKinney, Deputy Chief of Staff/White House Liaison
Timothy Noelker, General Counsel
Mike Terry, Deputy Chief Information Officer
Marie Murphy, Chief Information Security Officer
Colin Jones, Compliance Officer

October 30, 2020

Ms. Kathy A. Buller
Inspector General
Office of the Inspector General
The Peace Corps
1275 First St NE
Washington, DC 20526

Dear Ms. Buller:

Williams Adley is pleased to provide our support on finalizing the report for the performance audit we conducted to evaluate the effectiveness of the Peace Corps (PC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the Fiscal Year (FY) ending September 30, 2020.

The report details the results of our evaluation of the PC's information security program and practices. FISMA requires each agency Inspector General, or an independent external auditor, to conduct annual evaluations of their agency's information security programs and practices, and to report to the Office of Management and Budget (OMB) on the results of their evaluations. OMB Memorandum M-20-04 ("Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements") provides instructions for meeting this year's reporting requirements.

Our independent FISMA evaluation followed 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. In all other respects, our evaluation met the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

The objective for this independent evaluation was to determine if PC implemented an effective FISMA information security program and practices for the period October 1, 2019 to September 30, 2020 for its information systems, including the PC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We assisted the PC Office of Inspector General (OIG) in categorizing the identified findings for the CyberScope metrics. We based our work, in part, on a selection of agency-wide and system-specific security controls. Additional details regarding the scope of our independent evaluation are included in Appendix A, Scope and Methodology.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, PC established and maintained its

information security program and practices for its information systems for the five cybersecurity functions and eight FISMA metric domains. While the security program has been implemented across PC, we identified findings within all of the cybersecurity functions and FISMA domains.

We have made recommendation related to the challenges faced by PC that, if effectively addressed by PC management, should strengthen the PC information security program. PC management has provided us with a response to this FY 2020 FISMA audit report. Their response is included in the appropriate sections of this report. We did not audit management's response and, accordingly, do not express any assurance on it.

This report is issued for the restricted use of the OIG, management of the PC, and OMB. Williams Adley did not render an opinion on PC's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation to future periods or other information systems not included in our selection is subject to the risks that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate. We appreciate the opportunity to assist your agency with this evaluation. Should you have any questions, please call Mr. Tony Wang, Partner, at (202) 371-1397.

Williams, Adley & Company-DC, LLP

Washington, DC

Peace Corps Office of
INSPECTOR GENERAL

Final Report

Review of the Peace Corps' Information Security Program

October 2020

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) 2020.[1]

RESULTS IN BRIEF

The FY 2020 FISMA results are consistent with more than a decade of Peace Corps Office of Inspector General (OIG) reviews outlining concerns over the agency's management of IT security. Since 2009, OIG has reported in our statements on management and performance challenges that the Peace Corps has not implemented an effective information security program or achieved full compliance with FISMA.

The results of FY 2020 review which assess the agency's performance against a government wide maturity model, places the Peace Corps at Level 1, ad-hoc, or operating in a reactive manner. The Office of Management and Budget (OMB) expects the agency to be operating at Level 4, which is defined as managed and measurable. There are numerous FISMA findings that have been outstanding for over a decade and we continuously have noted repeated weaknesses related to people, processes, and technology. This year two of the more notable examples include:

- The backbone of the agency's IT infrastructure operating without undergoing the proper assessment and authorization; and
- Outdated IT assets operating without adequate protections.

These two examples are illustrative of the larger systemic weaknesses in the agency's information security program. Change at this level requires a serious and sustained undertaking with involvement and dedication from every level of the organization. The agency does not have the appropriate structure in place to promote effective planning, resources, and communications necessary for this holistic change.

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

During FY 2020, the Peace Corps program suffered significant upheaval, and the agency underwent substantial changes to its operations: the data center was relocated, the headquarters building moved, and all Peace Corps Volunteers were recalled due to the ongoing COVID-19 pandemic. In dealing with these major shifts in operations, the Peace Corps focused on keeping the agency operating without interruptions. However, this exposed the agency to serious information security risks. While the Peace Corps has not suffered a catastrophic operational or cybersecurity failure, the risk of such an event remains high.

TABLE OF CONTENTS

BACKGROUND

THE PEACE CORPS

The Peace Corps is an independent Federal agency that's 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' 58 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.

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 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 2020 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 2020.[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 Peace Corps' compliance with the provisions of FISMA.

RESULTS

OVERVIEW

The FY 2020 FISMA results are consistent with more than a decade of Peace Corps Office of Inspector General (OIG) reviews outlining concerns over the agency's management of IT security. Since 2009, OIG has reported in our statements on management and performance challenges that the Peace Corps has not implemented an effective information security program or achieved full compliance with FISMA.

The results of the FY 2020 review, which assessed the agency's performance against a government wide maturity model, place the Peace Corps at Level 1, ad-hoc, or operating in a reactive manner. OMB expects the agency to be operating at Level 4, which is defined as managed and measurable. There are numerous FISMA findings that have been outstanding for over a decade, and we continuously have noted repeated weaknesses related to people, processes, and technology. This year two of the more notable examples include:

- The backbone of the agency's IT infrastructure operating without undergoing the proper assessment and authorization; and
- Outdated IT assets operating without adequate protections.

These two examples are illustrative of the larger systemic weaknesses in the agency's information security program. Change at this level requires a serious and sustained undertaking with involvement and dedication from every level of the organization. The agency does not have the appropriate structure in place to promote effective planning, resources, and communications necessary for this holistic change.

During FY 2020, the Peace Corps program suffered significant upheaval and the agency underwent substantial changes to its operations: the data center was relocated, the headquarters building moved, and all Peace Corps Volunteers were recalled due to the ongoing COVID-19 pandemic. In dealing with these major shifts in operations, the Peace Corps focused on keeping the agency operating without interruptions. However, this exposed the agency to serious information security risks. While the Peace Corps has not suffered a catastrophic operational or cybersecurity failure, the risk of such an event remains high.

AUTHORIZATION PROCESS FOR THE GENERAL SUPPORT SYSTEM

The General Support System (GSS) is the backbone for the agency's IT infrastructure and it is currently operating without undergoing a full and comprehensive system security review to ensure that all proper controls are in place. Without a full assessment and authorization, the Peace Corps' has put its data and systems at risk.

History of the GSS

The GSS is a collection of platforms and systems that form a networked infrastructure to support the Peace Corps' data processing needs. This infrastructure includes hardware, software, applications, databases, communications, and Internet access to support the agency's overall mission and daily operations.

Prior to FY 2019, the GSS was made up of servers located in the Peace Corps headquarters building on 20th Street NW in Washington, DC and at overseas posts and domestic recruiting offices (referred to as "the original GSS" in this report).

In FY 2019, the Peace Corps undertook the largest change to the agency's IT infrastructure in over 7 years by moving the headquarters portion of the GSS offsite to a commercial data center (referred to as "the data center" in this report). In moving the data center, the agency failed to follow its own assessment and authorization process to ensure there were adequate security controls in place. This botched approach resulted in wasted time and resources (for more details see our FY 2019 report[5]). On September 12, 2019, the CIO authorized the new data center system a 1-year authorization to operate (ATO). However, this ATO was contingent on the maintenance and management of the security posture of the system.

Concurrently with the data center move, the agency also physically changed headquarters locations at the end of 2019. With this move, the remaining headquarters portion of the original GSS was dismantled and assets were either retired or relocated to the new data center or to the new headquarters building on First Street NE in Washington D.C. The transition to the new headquarters was completed in December 2019.

Requirements

NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, requires all new systems to undergo an assessment of security controls to ensure effectiveness. Specifically, the guidance outlines six steps – security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring – to develop Federal information systems with a risk-based approach to security.

Furthermore, NIST SP 800-37 requires ongoing monitoring to maintain situational awareness about the security and privacy postures of the information system. It also requires determining the impact these changes have on the organization, as it aligns with the larger enterprise risk management framework.

The Peace Corps Infrastructure Not Properly Reviewed

When the initial ATO was granted for the data center in September 2019, there were three contingency requirements. Specifically:

1) Maintenance of the current information system's security posture;
2) Management of Plan of Action and Milestones (POA&M) in accordance with Peace Corps policy; and
3) Maintenance of the System Security Plan (SSP) in compliance with the Continuous Monitoring phase of the Risk Management Framework lifecycle.

However, we determined that the agency did not fulfill these requirements and therefore invalidated the ATO.

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

Information System Security Posture is At Risk
Overall, the Peace Corps lacks an effective information security posture. While the Department of Homeland Security considers Level 4, Managed and Measurable, to be an effective level of security, the Peace Corps has only reached an overall FISMA maturity level of Level 1, Ad-hoc. Within the five functional areas, the highest rating the Peace Corps has achieved is Level 2, Defined, for its incident response program.

Year after year the Peace Corps has not been able to fully implement an agency-wide risk management program to manage risks across the organization at all three levels (entity, business process, and system). In FY 2020, the agency began to make progress initiating the risk management process at the entity level by reaching out to each business unit to identify potential risks and beginning to develop the risk registry. However, the registry failed to identify any risks from OCIO.

Unresolved Plan of Action and Milestones Issues
The agency did not document and track all weaknesses identified from the independent security assessment report (SAR) within POA&Ms, which outline steps, including milestones, on how the agency intends to remediate the identified weaknesses and are critical to ensuring the security infrastructure remains strong.

The Peace Corps POA&M Management Guide states that weaknesses identified in the security control assessment and vulnerability scanning must result in a POA&M being created within 30 days of identification, unless the remediation can be taken within that 30-day period.

The data center SAR identified a number of failed security controls and critical and high vulnerabilities that needed to be remediated. The agency created 14 POA&Ms to address these weaknesses. However, after a year, these POA&Ms have not been completed.

Furthermore, the agency did not capture all of the identified weaknesses in those 14 POA&Ms. Based on the agency's policy it is possible that corrective actions were taken within 30 days and therefore POA&Ms were unnecessary. However, the agency did not maintain updated system security documentation for the data center, which prevented us from being able to determine if proper corrective actions were taken in a timely manner.

Maintenance of the System Security Plan and the System Boundary
The Peace Corps did not maintain the security plan in accordance with NIST requirements and Peace Corps policy. After the 1-year ATO was granted for the new data center, the Peace Corps quickly began adding new infrastructure components to this system, creating a new, larger GSS system (referred to as "the new GSS" in this report). Specifically, when the data center was granted an ATO, all of the components were located at one facility in a single location; however, as of June 2020, the new GSS had components that supported over 60 different locations, including the data center, the new headquarters building, all overseas posts, and 3 domestic recruiting offices.

In making these major changes to the footprint of the data center system and growing the boundary exponentially, the agency was required to assess additional controls to properly evaluate the risks that were introduced to the environment or evaluate the impact this had on the organization. However, the Peace Corps did not start the independent assessment until June

2020, over 6 months after these changes were implemented within its current production environment.

Unfortunately, this is not the first time the agency has circumvented the assessment and authorization process. For example, in FY 2016, Peace Corps Medical Electronic Documentation & Inventory Control System (PCMEDICS), which stores highly sensitive Volunteer Personal Health Information, did not go through the appropriate security assessment and authorization process before being brought into production.[6] 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. And, as already mentioned, in FY 2019, the agency failed to follow the correct steps when bringing the data center into production.

Ensuring the GSS is adequately developed and implemented is critical since it supports all business functions. The absence of following the assessment and authorization process puts all Peace Corps information systems and sensitive data at an unknown risk.

NO SUPPORT PLAN FOR IT ASSETS AT END OF LIFE

By having outdated, unsupported hardware and software in its environment, the Peace Corps did not provide adequate protections for the agency's information and information systems. This issue was also compounded since the Peace Corps lacks a complete picture of its IT environment. Without properly managing and supporting hardware and software assets, the Peace Corps has been left vulnerable and open to threats and malicious attacks.

Outdated, Unsupported IT Assets Definition

When an IT asset reaches its "end of life" this refers to the date when a vendor no longer provides automatic fixes, updates, or online technical assistance. Vulnerabilities in the assets that are discovered after this date will not be fixed. Hackers and malicious actors target these end of life assets to exploit known vulnerabilities, as it provides an easier entry into an organization's IT infrastructure.

Requirements

NIST requires software and hardware to be maintained in a manner that provides adequate protection for the organization. Specifically, NIST SP 800-64, Security Considerations in the System Development Life Cycle, states that security considerations are relevant to the legacy systems and should be applied and documented to ensure security controls are in place and functioning effectively to provide adequate protections for the information and the information system. Furthermore, NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, states that the organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

[6] Review of Peace Corps Information Security Program for FY 2016, November 10, 2016.

IT Assets Operating without Adequate Protections

The Peace Corps did not provide adequate protections for its information and information systems. Specifically, the agency had outdated, unsupported hardware and software in its environment. These issues were widespread across the infrastructure from individual computers, assets at overseas posts, and centralized servers within the Peace Corps environment, including critical systems like the financial system.

At the end of FY 2019, the agency made the transition to a new data center and upgraded many of its infrastructure components, however, it also brought along approximately 40 assets that would be obsolete in less than 6 months. The agency did not use this transition time to upgrade or remove these end of life assets from the network, despite the vendor announcing the end of life date over a year prior to the data center being brought into production.

Furthermore, the agency failed to provide adequate support to these outdated assets. While the vendor offered "a last resort option for customers who need to run certain legacy products past the end of support," the agency did not contract for these services until over 6 months after these assets reached their end of life dates.

These outdated and unsupported assets throughout the Peace Corps environment underscore the Peace Corps' lack of a complete picture of its IT environment. The agency does not have an automated or centralized tool to track, monitor, and reconcile the assets within its production environment. They rely on multiple different tools and do not have a process to reconcile the data to ensure accuracy.

REASON FOR AN INEFFECTIVE INFORMATION SECURITY PROGRAM

While the agency has attempted to make improvements to the policies, procedures, and technology, the Peace Corps remains at an ad hoc level, or operating in a reactive manner. Change at this level requires a serious and sustained undertaking with involvement and dedication from every level of the organization. The agency does not have the appropriate structure in place to promote effective planning, resources, and communications necessary for this holistic change. Furthermore, the agency has continued to make decisions for business convenience without understanding the information security risk or the impact to the entire agency. Despite successive years of problems there is an overall lack of accountability for achieving an effective information security program.

In dealing with the major shifts in operations that occurred in FY 2020, the agency focused on keeping the agency operating without interruptions. However, this exposed the agency to serious information security risks.

Lack of Planning

The agency's data center and headquarters relocations were multi-year projects that should have allowed for adequate time to ensure the proper assessment and authorization processes were followed. While our FY 2019 report[7] identified a lack of planning for the migration of the data center, the agency did not heed the warning, and improvements were not seen in FY 2020. When the data center was granted an ATO, it was only for one year. However, this ATO expired prior to the Peace Corps getting the new GSS through the assessment and authorization process,

[7] FY 2019 Review of the Peace Corps' Information Security Program

leaving the agency operating without an approved GSS. The agency failed to adequately plan to ensure that the assessment and authorization process was given enough time to prevent this lapse in coverage.

This lack of planning is also evidenced in the Peace Corps having end of life assets in the environment without support to remediate IT security vulnerabilities. Vendors who supply the agency's hardware and software assets announced end of life dates for their products years in advance to allow for organizations to plan transitions. In one example, the vendor provided 16 months advanced notice for a product's end of life date, but the agency was not able to remove approximately 170 assets before that deadline. Furthermore, the Peace Corps did not initiate communications to provide extended security updates for these end of life assets until after the expiration had already occurred and the support contract was not put in place until 6 months after the deadline.

Lack of Resources

Improvements to the agency's IT security posture requires collaboration from all levels of the organization. The chief information security officer (CISO) and her staff are responsible for developing, 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 group has struggled to maintain full staff capacity and recruit personnel with the appropriate knowledge, skills, and abilities to promote a strong security posture.

IT security responsibilities extend beyond the CISO and throughout the other parts of OCIO. The OCIO is responsible for the overall design and operations of the IT infrastructure, including the day-to-day functionality of the network. While OCIO plays a significant role in the agency's security posture, the individual groups within the office do not understand the impact that their operational decisions have on the agency's security posture.

Furthermore, IT security responsibilities extend beyond OCIO, each office within the agency plays a role in ensuring the IT security position of the agency. The agency needs to promote an understanding of these responsibilities through continuous and comprehensive role-based training.

Lack of Communications and Insufficient Enterprise Risk Management Program

Information security decisions that impact the agency's overall risk posture have not been made at the correct level. In July 2019, the agency established the Enterprise Risk Management Council with the main responsibility of reviewing, evaluating, and monitoring opportunities and risks to the agency's ability to achieve its' mission and goals. Peace Corps senior leadership stated that this council is still in the very early stages and the group is focusing on completing risk registries for each program office. While we previously mentioned that OCIO does not have a formal registry created, OCIO senior leadership team stated that they have an internal registry that focuses on the risks from the system perspective.

Despite this informal system-focused risk registry, substantial changes to the information security infrastructure and end-of-life assets operating without proper vendor support were not elevated to the Enterprise Risk Management Council or Peace Corps' senior leadership. The Council is part of the agency's efforts to implement an Enterprise Risk Management Program. In our FY 2019 review we noted that the lack of a fully implemented program prevented the agency

from identifying risks that could impact the agency's ability to fulfill its mission and conduct critical business processes. In this case, the CIO did not perceive these issues as having risk to the whole agency. However, changes at this magnitude and allowing obsolete and unsupported assets in the environment should have been communicated since it created a higher risk that would impact the agency's ability to function and meet its goals. Such communications are critical, particularly in the absence of a fully implemented Enterprise Risk Management (ERM) program.

Lack of Accountability

Lastly, there are few repercussions for failing to meet security standards. The Peace Corps is dependent on the IT infrastructure functioning. To ensure that business could operate as usual, when the agency failed to get the new GSS through the assessment and authorization process on time, it accepted having unreviewed systems in the infrastructure. By accepting the unauthorized GSS, the agency put its systems, employees, and Volunteers at risk. This scenario has been repeated for successive years but it's not clear those responsible at an individual or organizational level have been held accountable for poor performance.

IMPACT TO AGENCY

The continued lack of improvement to the health of the agency's information security program leaves sensitive data vulnerable and exposes the Peace Corps network infrastructure to attacks and disruptions.

The consequences of a weak information security program are real. 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. While the Peace Corps environment has similar IT security weaknesses to those that led to the OPM breach, the Peace Corps 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 Director appoint the chief information security officer to serve on the Enterprise Risk Management Council as a voting member.

3. OIG recommends that Peace Corps management enhance the communications protocols with different offices to ensure roles and responsibilities are clearly communicated and risks are consistently identified and communicated from system, business process, and entity levels.

4. OIG recommends that Peace Corps management add an IT security performance element to the annual performance plans for all staff members who have a role with IT security. This should include all system owners and staff members who have roles and responsibilities in managing and protecting Peace Corps sensitive data and information systems.

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 2020 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 2020:

- Peace Corps General Support System (PCGSS)
- Peace Corps Case and Adjudication Tracking System (PCCATS)

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 June to October 2020. They performed the review in accordance 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.

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

- FY 2020 Inspector General FISMA Reporting Metrics
- 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-20-04 "Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements"
- NIST Special Publications and NIST Federal Information Processing Standard Publications
- Peace Corps Policies, Standards, Guides, and Standard Operating Procedures

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
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
SAR	Security Assessment Report
SP	Special Publication
SSP	System Security Plan

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, *Risk Management Framework for Information Systems and Organizations*
  - iii. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - iv. NIST SP 800-64 Revision 2, Security Considerations in the System Development Life Cycle
  - v. FIPS Publication 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*

II. Protect

- a. Configuration Management
  - i. NIST SP 800-128, *Guide for Security Focused Configuration Management of Information Systems*
  - ii. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- 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. OMB M-11-11
- c. Security and Privacy Training
  - i. NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
  - ii. OMB Circular A-130

III. Detect

- a. Information Security Continuous Monitoring

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

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

IV. Respond

a. Incident Response

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

V. Recover

a. Contingency Planning

i. NIST SP 800-53 Revision 4, *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

MEMORANDUM

To: Kathy Buller, Inspector General

Through: Angela Kissel, Chief Compliance Officer

From: Scott Knell, Chief Information Officer

Date: October 23, 2020

CC: Jody K. Olsen, Director
Michelle K. Brooks, Chief of Staff
Matthew McKinney, Deputy Chief of Staff/White House Liaison
Carl Sosebee, Senior Advisor to the Director
Timothy Noelker, General Counsel
Michael Terry, Deputy Chief Information Officer
Marie Murphy, Chief Information Security 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 2020

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 2020 given to the agency on October 9, 2020.

The Peace Corps is committed to continuing to build and strengthen its information security and organizational risk management programs. Over the past year, the agency has initiated or deployed shared security services like EINSTEIN (E3a), Continuous Diagnostics and Mitigation (CDM), and Trusted Internet Connection (TIC). Fiscal Year 2020 also saw the implementation of robust disaster recovery (DR) and virtual private networking (VPN) solutions that improved connectivity and resilience. In order to address cybersecurity related staffing challenges, the agency awarded a contract temporarily increasing its information security staff levels over that of

prior fiscal years. Equally as important, prior Office of Inspector General recommendations were implemented, like providing risk management training to senior leadership and adding the chief information security officer to the Senior Policy Committee and Technical Advisory Board. Although the Peace Corps does not concur on all of the OIG recommendations issued within this report, the agency finds them reasonable and will take action to address the issues at the core of those 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.

Do Not Concur
Response: 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.

Documents to be Submitted: N/A

Status and Timeline for Completion: N/A

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 Director will appoint the chief information security officer to serve on the Enterprise Risk Management Council as a voting member.

Documents to be Submitted:
- Updated Enterprise Risk Management Council Charter

Status and Timeline for Completion: February 2021

3. OIG recommends that Peace Corps management enhance the communications protocols with different offices to ensure roles and responsibilities are clearly communicated and risks are consistently identified and communicated from system, business process, and entity levels.

Concur
Response: The agency will utilize the enterprise risk management executive secretariat to implement communication protocols with different offices to ensure roles and responsibilities are clearly communicated and risks are consistently identified and communicated from system, business process, and entity levels. This process will be discussed with the enterprise risk management council at the next council meeting.

Documents to be Submitted:

- Enterprise Risk Management Council Notes indicating communication plan discussion.
- Outline of risk communication protocols.

Status and Timeline for Completion: February 2021

4. OIG recommends that Peace Corps management add an IT security performance element to the annual performance plans for all staff members who have a role with IT security. This should include all system owners and staff members who have roles and responsibilities in managing and protecting Peace Corps sensitive data and information systems.

Concur
Response: The Office of the Chief Information Officer will coordinate with the Office of Human Resources to add an IT security performance element to the annual performance plans for all staff members who have a role with IT security.

Documents to be Submitted:

- Example of an updated performance plan that includes the added IT security performance element.
- List of positions with added IT security performance element in performance plans.

Status and Timeline for Completion: February 2021

APPENDIX F: OIG COMMENTS

OIG is disappointed with the agency's nonconcurrence on recommendation 1, to have the chief information security officer (CISO) run an independent office, and urges agency management to reconsider. Over the last 8 years, the agency has failed to adequately prioritize information security. It is critically necessary to provide the CISO with more independence to elevate information security risks and resource needs to agency senior executives. Our FY 2019 FISMA review found a lack of understanding of how IT security affects critical business operations and recommended that the CISO be integrated into the senior executive group. Regrettably, in our FY 2020 review, we continued to find a lack of prioritization and understanding of information security and how it is integral to business operations. While the agency has worked to implement some information security initiatives, these individual actions fall short of what is required.

The inadequacy of the current structure in the Peace Corps is highlighted by repeated findings in our reports. During the last 8 years, OIG has repeatedly reported how the agency has prioritized programmatic and operational needs to the detriment of information security. For example, the CIO has repeatedly circumvented the assessment and authorization process allowing multiple systems, including the General Support System, to be operational without completing critical steps in the authorization process. By elevating the CISO position and separating the OCIO programs and operations from the security functions, the agency would allow each priority to have equal footing at the senior leadership level. Furthermore, this would ensure that cybersecurity risks are fully understood and evaluated when making key business decisions, which would ensure the protection of the agency's reputation, operations, and ability to keep Volunteers' sensitive data safe and secure.