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
Anne Hughes, Chief Compliance Officer

From: Kathy A. Buller, Inspector General

Date: October 31, 2019

Subject: Review of the Peace Corps' Information Security Program for FY 2019

Please find attached the annual Report on the Peace Corps' Information Security Program. This review was conducted by Williams Adley to assess the effectiveness of the security controls and practices. The report makes 5 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.

The agency response to the report and the five recommendations is estimated to be received by November 20, 2019. When provided, the report will be updated to include the agency's response in Appendix E. OIG comments on the agency's response will be included in Appendix F.

cc: Matthew McKinney, Deputy Chief of Staff/White House Liaison
Robert Shanks, General Counsel
Mike Terry, Deputy Chief Information Officer
Marie Murphy, Chief Information Security Officer
Angela Kissel, Compliance Officer

Peace Corps Office of
INSPECTOR GENERAL

Final Report

Review of the Peace Corps' Information Security Program

October 2019

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) 2019.[1]

RESULTS IN BRIEF

While in FY 2018 the Peace Corps made strides to improve its IT security process, in FY 2019 the agency took steps that undermined the progress it had made. While undergoing the largest change to the agency's IT infrastructure in over 7 years, moving the data center offsite, IT security was neglected. For example, the agency failed to ensure that adequate security controls were designed.

There are several FISMA findings that have been outstanding for over 8 years and the agency has struggled to implement corrective actions. Some of the more egregious examples include:

- Disregarding key Federal regulations for access control,
- Inability to protect sensitive data from insider threat,
- Lacking a complete understanding of the Peace Corps' IT environment, and
- Failure to ensure that critical business processes and the IT environment can be recovered in event of a disaster.

These problems are crippling the IT security program and pose a significant risk to the agency. These conditions exist because there is a lack of understanding of how IT security affects critical business operations. The agency, including the leadership of OCIO, has taken a hands-off approach, and those with the knowledge have not been empowered to make decisions.

The consequences of a weak IT security program are real. In the Federal government, OPM faced a major compromise to their network and sensitive information in 2014. While the Peace Corps environment has similar IT security weaknesses that led to the OPM breach; the Peace Corps has not adequately integrated IT security with business operations to ensure the protection of its operations, reputation, and ability to keep Volunteers safe.

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

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 information technology (IT) services and solutions that enable the Peace Corps to achieve its mission and strategic goals. The agency's global IT infrastructure provides services to a user base of nearly 4,000 full-time and part-time personnel distributed throughout the world. OCIO's IT services affect both domestic Peace Corps staff—located at the Washington, D.C. headquarters, three regional recruiting offices, and remote locations connected via the Virtual Private Network —and international staff located at the Peace Corps' 58 posts worldwide.

FEDERAL INFORMATION SECURITY MANAGEMENT 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-19-02, Oct..2018.

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 2019 IG FISMA Metrics also mark a continuation of the work that OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency began in FY 2015 to move the IG assessments to a maturity model-based approach. The FY 2019 IG FISMA Metrics provide maturity models for all five security functions and reorganize the models—provided in the prior year—to be more intuitive. This alignment with the Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the IG metrics process while providing agencies with a meaningful independent assessment of the effectiveness of their information security program 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 2019.[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

Since 2009, the Peace Corps Office of Inspector General (OIG) has reported in our statements on management and performance challenges that the Peace Corps has not achieved full compliance with FISMA or implemented an effective IT security program. There are several FISMA findings that have been outstanding for over a decade and the agency has struggled to implement corrective actions.

The FY 2019 maturity model puts the Peace Corps at an ad hoc level, or operating in a reactive manner, while OMB expects the agency to be operating at Level 4, managed and measurable. We found problems relating to people, processes, and technology. These problems exist because there is a lack of understanding of how IT security affects critical business operations. The agency, including the leadership of OCIO, has taken a hands-off approach, and those with the knowledge have not been empowered to make decisions.

The Peace Corps has continued to disregard key OMB and NIST requirements and OIG recommendations. While the agency has not suffered a catastrophic operational or cybersecurity failure, the risk of such an event remains high. The agency's failure to implement an effective risk management program further compounds the risk.

While in FY 2018 the Peace Corps made strides to improve its IT security process; in FY 2019 the agency took steps that undermined the progress it had made. While undergoing the largest change to the agency's IT infrastructure, moving the data center offsite, IT security was neglected.

Some of the more egregious examples of the long outstanding problems include:

- Disregarding key Federal regulations for access control,
- Inability to protect sensitive data from insider threat,
- Lacking a complete understanding of the Peace Corps' IT environment, and
- Failure to ensure critical business processes and the IT environment can be recovered in the event of a disaster

AUTHORIZATION PROCESS FOR THE NEW DATA CENTER

While undergoing the largest change to the agency's IT infrastructure in over 7 years, moving the data center offsite, the agency failed to follow their own process to ensure the data center had adequate security controls in place, formally called the assessment and authorization process. According to the CIO, the decision to move the data center occurred prior to his joining the agency in January 2017. In May 2018, the Peace Corps entered into a contract with an outside vendor to help with the design and implementation of the new data center.

Requirements

Prior to introducing a new system into the agency's IT environment, the Peace Corps should assess the security controls of the system to ensure effectiveness. NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, 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.

Botched Authorization Process

One of the first steps of the assessment and authorization process is to determine the risks to the system; however, the agency has yet to complete this assessment over 18 months after the contract began and after agency data has been moved into the new data center. The basis for identifying risks is to ensure the system design adequately protects the information in the system by selecting the appropriate security controls from the catalog of options.

After the appropriate security controls have been identified, the next steps in the process are to implement these controls on the new system, document the controls in a system security plan, and have these controls tested by an independent assessment team. The Peace Corps failed the independent assessment because OCIO could not identify or demonstrate what IT security controls it had taken. The independent assessment team tried to determine if the issues were just incomplete documentation, but they stated in their report that this was not the case, there was a lack of understanding of the security control requirements. Specifically, the report stated:

> Attempts to address the incomplete description of security controls in the [security documentation] were made during the interviews to ascertain whether the security control requirements were known and being implemented, and that only the documentation was incomplete – this was clearly not the case. It was clear that the documentation was not developed, and the requirements were not understood.

This May 2019 assessment concluded that 135 out of 135 controls failed and the independent assessment team concluded that the risk of putting the new data center into production was high and recommended that the agency not begin operations.

It took the agency over 6 weeks to correct the issues identified and resubmit for a second independent assessment in August 2019. This review identified that over half of the controls failed (48 of the 91 controls); however, the independent assessment team concluded that risk had been reduced to a medium level and recommended that the agency could begin operations. The CIO authorized the new system on September 12, 2019.

ACCESS CONTROL

Typically, the first line of defense for preventing unauthorized access to systems is an established process to identify and authenticate that users are allowed.

Requirements

Homeland Security Presidential Directive-12 (HSPD-12) established requirements for a common identification standard for Federal employees and contractors. According to HSPD-12, the benefits of secure and reliable forms of identification issued by the Federal Government include enhancing security, increasing government efficiency, reducing identity fraud, and protecting

personal privacy. OMB Memorandum 11-11 states that agencies must upgrade existing physical and logical access control systems at the beginning of FY 2012.[5]

Neglecting Federal Regulations

Over 7 years after the required implementation date, the Peace Corps is still not compliant with HSPD-12. When the agency completes the physical headquarters move, the agency should be closer to compliance. However, full compliance will not be achieved until multi-factor authentication for both physical and logical access is implemented for all Peace Corps system users and physical locations.

PROTECTION OF SENSITIVE DATA

Sensitive information, including personally identifiable information (PII), protected health information (PHI), and detailed financial information should be protected from inappropriate dissemination.

Requirements

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, outlines the steps that agencies should take to ensure that sensitive information is identified and protected in transit, at rest, from being taken, and/or used without authorization.

Incapable of Protecting Sensitive Data

The Peace Corps does not have a robust data protection and privacy program. The Peace Corps has not identified all locations where sensitive data is located or implemented controls to ensure that unauthorized staff do not have access. Additionally, the agency is unable to determine if personnel have taken that sensitive information off the network. Lastly, the agency has not developed specific training for the IT personnel who have elevated system privileges that allow them to handle, work with, and support offices that process sensitive information to ensure the correct protections are taken.

DEFINING THE IT ENVIRONMENT

In order to understand the risk to information security, the organization must first define its environment, including what hardware and software assets it owns and how these systems interconnect with each other. Having an understanding of where the agency's IT boundaries lie is critical to knowing how to protect the information residing in the Peace Corps network.

Requirements

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, outlines that agency should have a documented inventory of information system components that accurately reflects the environment.

Additionally, NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, also states that agencies should establish terms and conditions with other

[5] OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, Feb. 2011.

organizations that own, operate, and/or maintain external information systems that house agency data to ensure this information is adequately protected.

Lacking a Complete Understanding of the IT environment

The Peace Corps does not have a complete picture of its IT environment. While the agency has purchased tools to track hardware, software, and information systems, the agency continues to struggle with having accurate records and listing all assets. The tools purchased do not interact, and there is no process to reconcile information to ensure it is accurate. Additionally, the agency does not have the ability to detect or remove devices that are not authorized to be on the network.

Furthermore, approved information system security documentation outlines interconnections to systems that do not exist in the Peace Corps environment. Lastly, the agency does not have a process to assess and implement controls for external Federal systems that the Peace Corps utilizes as part of their business operations.

CONTINGENCY PLANNING

Being able to timely recover the entire IT environment or individual systems after a disruptive event is essential. The primary purpose of contingency planning is to give attention to events that have the potential for significant consequences, prioritize the restoration of mission-critical systems, and ensure the Peace Corps can return to normal operations as quickly as possible.

Requirements

NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, requires agencies to develop, review, and test individual system contingency plans to determine the effectiveness of the plan and the organizational readiness to execute the plan.

Furthermore, the Peace Corps Domestic Infrastructure Disaster Recovery Plan, which covers the restoration of critical agency systems that require activation of that agency's alternate IT processing site, states that "the Business Continuity Plan Coordinator will review and update the entire Domestic Infrastructure Disaster Recovery Plan whenever there is a significant change or at least annually to make sure that everything in it is current and correct."

Longstanding Failure to Ensure Operations can be Recovered

For the last 3 years the agency has been operating without a viable contingency plan for if one or more of its information systems were to become inoperable. The agency's disaster recovery plan, which covers the restoration of critical agency systems that require activation of that agency's alternate IT processing site, has not been updated since 2010. However, the agency's critical systems have changed and the alternative processing site has not been in operation for approximately 2 years. Furthermore, the individual system contingency plans, which cover the specific actions that must be taken to recover the data and functionality of a specific system, have not been tested recently to ensure that a full recovery is even possible. For example, the agency's financial system has not been tested since April 2016.

REASON FOR AN INEFFECTIVE IT SECURITY PROGRAM

The weak security program exists because there is a lack of understanding how IT security affects critical business operations. The agency, including the leadership of OCIO, has taken a hands-off approach, and those with the knowledge have not been empowered to make decisions.

Enterprise Risk Management Framework

The July 2016 memo, OMB M-16-17, "OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control," requires agencies to have an enterprise risk management framework established. However, the agency has not been successful in establishing this framework. The agency has not identified risks that could impact the agency's ability to fulfill its mission and conduct critical business processes, including processes related to finances, physical security, information security, and property management. Furthermore, the agency has not determined their risk tolerance and how they plan to communicate this approach to all necessary internal and external stakeholders.

The agency established "organizational risk management" as one of its six management objectives in its FY 2018 – 2022 Strategic Plan and set a goal of developing policy, procedures, and an agency-wide risk profile that would be used in decision making by the end of FY 2019. The agency has only taken the first step in approving the policy and developing a charter for a governing council. Senior agency officials have stated that efforts to move ERM forward have stalled because this is an "other duty as assigned" and not one person is fully dedicated to the project. The agency planned to assign this initiative to the Deputy Director; however, the candidate for this position has not yet been confirmed by Congress.

Furthermore, IT security has not been adequately integrated into business operations, as the CIO is not part of the agency's senior policy committee (SPC), the group with oversight responsibility for the Peace Corps Manual. The SPC is responsible for ensuring that the Manual, the Peace Corps' authoritative policies governing the operations of the agency, accurately reflects applicable law and policy, and coordinates the oversight and approval for procedures that implement Manual policies.

Hands-off Approach

The agency, including the leadership in OCIO, has taken a hands-off approach to IT security. Since 2009, OIG has reported in our statements on management and performance challenges that the Peace Corps has not achieved full compliance with FISMA or implemented an effective IT security program. For example, there are several FISMA findings that have been outstanding for over a decade and the agency has struggled to implement corrective actions. In another example of this hands-off approach, at the end of last year OIG briefed the agency that none of their contingency planning documentation reflected operations; however, no changes were made to ensure the agency could recover in the event of a system failure.

The Peace Corps Manual Section 129, Office of the Chief Information Officer: Organization, Mission, and Functions, states that the mission of OCIO is to provide advice and other assistance to the Director and senior management to ensure that IT is acquired and information resources are managed in a manner that implements the policies, procedures, and the priorities established by the Director.

Senior agency management relied on the CIO to keep them updated on major IT security issues and any significant challenges related to the data center move. However, on July 17, 2019, OIG was the first to inform senior agency management of the issues related to the May 2019 security assessment. Prior to our meeting, they had not been informed of problems that would impact the viability of moving the data center into production.

While the CIO stated that he is responsible for granting permission for the new data center to go into production; he also stated that he was not involved in the design and implementation of the security infrastructure and relied on his staff to ensure that the needed steps were taken. He was briefed by his staff on IT security related to the new data center on two occasions: once on July 19, 2019 and once on September 12, 2019. OCIO had no plan for the possibility of not completing the data center move before the Peace Corps moves out of their headquarters location in December 2019. The agency did not have a back-up plan on how to mitigate the risk of the data center move being delayed.

Unempowered CISO

IT security needs a voice within senior management, someone to raise concerns at the high enough level to make change and ensure IT security is implemented in the appropriate form. According to Interim Policy Statement 1-17, Information Security Program, the Chief Information Security Officer (CISO) is responsible for developing, documenting, and implementing an agency-wide IT security program including the development of policies, procedures, and control techniques to address all applicable requirements for protecting Peace Corps information and information systems. Yet the CISO is not on the SPC and does not have a meaningful role in ensuring proper IT policy development and implementation. Moreover, the CISO is not otherwise empowered to effectively perform the CISO function.

Furthermore, the Peace Corps has a group called the Technical Advisory Board (TAB) to provide executive direction and business-centered guidance for investment of agency resources (human, financial, and capital) in information technology, while ensuring an equitable process under which agency resources are allocated. The TAB is led by the CIO and Deputy CIO; however, the CISO is not a member of this group, and in order to attend meetings must get invited by a TAB member and have prior consent of all TAB members. While this group is responsible for reviewing and assessing the adequacy of existing or proposed information technology investments and prioritizing them using a standard set of criteria, it does not appear that security has been incorporated into the process. Over the years, we have seen security controls circumvented to introduce unvetted systems, software, and processes, and this has been with senior leadership's knowledge and lack of security considerations.

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 IT security program are real. In the Federal government, OPM faced a major compromise to their 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, system authorizations out of date, and poor patching. While the Peace Corps environment has similar IT security weaknesses 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.

Authorization Process for the Data Center

Without considering information security or following the appropriate processes, the data center move created unnecessary costs and could still potentially cost the agency close to a million dollars or more. Having to repeat the independent assessment process, added a significant amount of time to an already delayed project. Additionally, the independent assessor had to divert attention from their regular workload to focus on this project for two independent reviews. The agency also entered into the rental agreement with the new data center facility in September 2017; however, the contract to begin designing the data center did not begin until May 2018, and the approval to move production data was not granted until September 2019. The annual cost of the new data center space is approximately $315,000 for the first year and $260,000 for subsequent years. OIG approximates that this is $300,000 of wasteful spending.

If OCIO cannot complete the data center move before the end of December 2019, the agency will need to spend approximately $800,000 per month to maintain the rent of the current headquarters building.

Access Control

Without two-factor authentication, as required by HSPD-12, outside threats could have a more readily available path to Peace Corps information systems. Ensuring that it is as difficult as possible for individuals to gain access to the network will prevent less skilled cyber criminals from accessing the agency's information. The Peace Corps has two-factor authentication partially implemented, but, until the agency completes the process, it is like locking the front door and leaving the windows open.

Protection of Sensitive Data

Without the identification and protection of sensitive data, the Peace Corps is at risk of this information being removed without the agency's consent. The Peace Corps systems house Volunteer and staff PII, such as social security numbers, home addresses, and Volunteer site locations, and Volunteer PHI, such as medical records and sexual assault information. This information is at risk of being taken off the network and sold on the Dark Web or utilized by foreign operators to gain leverage over Volunteers and staff around the globe.

Defining the IT Environment

Without a complete understanding of the environment, the Peace Corps cannot effectively protect all IT assets. This leaves software and hardware unpatched, or without current updates to security controls, giving hackers an unimpeded path to the agency's data. Additionally, for the hardware and software that the Peace Corps does know about, there are no defined standards on what these systems should look like to ensure that the infrastructure is as secure and uniform as possible.

Contingency Planning

Without accurate contingency plans and regular testing of these plans, the ability for the Peace Corps to recover in the event of an information system outage is compromised. The recovery operations could take longer, cost more, and could result in the permanent loss of data. In the last few years, there have been at least two occasions where water fountains above the current data center leaked and caused flooding within the building. With one of those occasions the flooding reached the floor where the data center is housed. If the flooding had not been stopped, the agency would have faced a significant risk to its hardware and information. The Peace Corps does not have the plans in place to quickly and efficiently recover from such an event. The organization's critical business functions, including the ability to pay vendors, access Volunteer information and locations, and other data would be down for an unknown amount of time and potentially unable to be recovered.

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 Officer and the Chief Information Security Officer to serve on the Senior Policy Committee.

3. OIG recommends that the Director appoint the Chief Information Security Officer to serve on the Technical Advisory Board.

4. OIG recommends that the Director dedicate resources, with the knowledge, skills, and abilities, to fully implement a comprehensive Enterprise Risk Management program.

5. OIG recommends that the Director provide training to all senior management and Office of Chief Information Officer staff on risk-based, security focused approach, including FISMA framework and how it ties into business and IT operations.

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 2019 FISMA guidance from the 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 2019:

- Volunteer Information Database Application (VIDA),
- Consolidated Incident Reporting System (CIRS),
- Sunflower Enterprise System (SES),
- Peace Corps Emergency Notification System (PCENS)

The Peace Corps OIG contracted accounting and management consulting firm Williams, Adley & Company LLP-DC to perform the assessment of the Peace Corps' compliance with the provisions of FISMA. Williams Adley performed this review from May to October 2019. 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.

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

- FY 2019 Inspector General FISMA Reporting Metrics
- Public Law 113–283, FISMA
- OMB Circulars A-123, A-127
- OMB/DHS Memorandums issued annually on Reporting Instructions for FISMA and Agency Privacy Management
    - OMB M-19-02 "Fiscal Year 2018-2019 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. They 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

CISO	Chief Information Security Officer
DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive-12
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
PHI	Protected Health Information
PII	Personally Identifiable Information
SP	Special Publication
SPC	Senior Policy Committee
TAB	Technical Advisory Board

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 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - iii. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - iv. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Security Systems*
  - v. OMB M-19-02, *Fiscal Year 2018-2019 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: Anne Hughes, Chief Compliance Officer

From: Scott Knell, Chief Information Officer

Date: November 20, 2019

CC: Jody K. Olsen, Director
Michelle K. Brooks, Chief of Staff
Matt McKinney, Deputy Chief of Staff/White House Liaison
Carl Sosebee, Senior Advisor to the Director
Bob Shanks, General Counsel
Michael Terry, Deputy Chief Information Officer
Marie Murphy, Chief Information Security Officer
Angela Kissel, Compliance Officer
Joaquin Ferrao, Deputy Inspector General
Judith Leonhardt, AIG/Audits

Subject: Review of the Peace Corps' Information Security Program for FY 2019

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 2019 given to the agency on October 31, 2019.

The Peace Corps finds the OIG's recommendations reasonable, and while the agency does not concur on all the mitigation strategies suggested, it will take action to address the issues at the core of those recommendations. It should be noted that the agency does not accept several of the assertions that underpin those recommendations. In particular, those assertions that are not supported by available evidence, both included or omitted from consideration. Therefore, the Peace Corps does not accept the conclusion that it neglected IT security during its data center move or the assertion that senior leadership takes a hands-off approach to IT security.

Recommendation 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 seeks to ensure that the Chief Information Security Officer (CISO) is provided equal attention and consideration from the senior executive, as well as a degree of independence from the CIO. While the agency concurs with that premise, it differs on the approach to achieve those goals. Rather than moving the CISO to a new office, a number of changes will be undertaken to establish clear, redundant lines of communication between the CISO and senior executives. These steps will meet the aforementioned goals and maintain the close working relationship established between the staff that support the information systems and the cybersecurity professionals that support them.

Documents to be Submitted:
- Plan for CISO Engagement with Senior Leadership

Status and Timeline for Completion: January 2020

Recommendation 2
OIG recommends that the Director appoint the Chief Information Officer and the Chief Information Security Officer to serve on the Senior Policy Committee.

Do Not Concur
Response: The Peace Corps concurs that the Chief Information Officer should be a member of the Senior Policy Committee. However, the agency does not concur that the CISO should become a member of the SPC. The Chief Information Security Officer, serving as subject matter expert and advisor to the CIO, will be regularly consulted, as necessary in that capacity. It should be noted that within the Office of the CIO, the CISO and IT security staff directly support the development and maintenance of all IT related policy.

Documents Submitted:
- Updated SPC Charter with CIO Included in Membership

Status and Timeline for Completion: December 2019

Recommendation 3
OIG recommends that the Director appoint the Chief Information Security Officer to serve on the Technical Advisory Board.

Concur
Response: The Peace Corps will update its Technical Advisory Board (TAB) to establish the CISO role and responsibilities within that body.

Documents to be Submitted:

- Updated TAB Charter with CISO Included in Membership

Status and Timeline for Completion: December 2019

Recommendation 4

OIG recommends that the Director dedicate resources, with the knowledge, skills, and abilities, to fully implement a comprehensive Enterprise Risk Management program.

Concur

Response: The Peace Corps will dedicate resources to fully implement a comprehensive Enterprise Risk Management program.

Documents Submitted:

- Plan for Implementation of ERM Program

Status and Timeline for Completion: January 2020

Recommendation 5

OIG recommends that the Director provide training to all senior management and Office of Chief Information Officer staff on risk-based, security focused approach, including FISMA framework and how it ties into business and IT operations.

Concur

Response: The Peace Corps is committed to revamping its training program to better equip its leadership at all levels on cybersecurity and risk management. Specifically, training improvements will focus on the Cybersecurity Framework, FISMA, risk management and operational security.

Documents to be Submitted:

- CIO Training Plan

Status and Timeline for Completion: May 2020

APPENDIX F: OIG COMMENTS

OIG is seriously concerned with the agency's nonconcurrence on the recommendations of having the Chief Information Security Officer (CISO) be independent and serve as a part of the senior executive group. In FY 2019, the CISO was not part of the Senior Policy Committee, Technical Review Board, or Enterprise Risk Management Council Charter as a voting member. This indicates that the agency lacks understanding of the importance of cybersecurity at both agency and business process levels. Without truly considering the cybersecurity risks when making key business decisions, the Peace Corps risks failing to ensure the protection of the agency's reputation, operations, and ability to keep Volunteers' sensitive data safe and secure. We will evaluate the agency's implementation of our recommendations and the effectiveness of all FISMA domains in FY 2020.