PEACE CORPS

Office *of* Inspector General

TOGETHER WE MAKE A BETTER PEACE CORPS

Report on the Peace Corps' Information Security Program for FY 2016

November 10, 2016

PEACE CORPS
Office *of* Inspector General
TOGETHER WE MAKE A BETTER PEACE CORPS
202.692.2900 · OIG@PEACECORPS.GOV · WWW.PEACECORPS.GOV/OIG/CONTACTUS

Review of Peace Corps' Information Security Program

November, 2016

Background

The Federal Information Security Management Act (FISMA) requires federal agencies to establish effective security over their sensitive information and establish a program to protect information systems from unauthorized access, use, disclosure, modification, and other harmful impacts. In addition, FISMA requires that annually each Office of Inspector General (OIG) review its agency's information security program and report results to the Office of Management and Budget.

Objectives

Under OIG supervision, an independent public accounting firm, Williams, Adley & Company-DC, LLP, conducted this review to assess the effectiveness of the Peace Corps' information security program and to determine whether security practices in FY 2016 complied with applicable federal laws, regulations, and information security standards.

Results in Brief

OIG is concerned about the quality of the IT security program, especially considering the sensitive data that the Peace Corps maintains, such as health records and sexual assault incident information about Peace Corps Volunteers.

Our results demonstrate that the Peace Corps lacks an effective information security program because of problems related to people, processes, technology, and culture. Furthermore, OIG found weaknesses across all of the FISMA reportable areas. There are several FISMA findings that have been outstanding for over seven years and the agency has struggled to implement corrective actions.

One of the more significant deficiencies is that the Peace Corps does not have a robust agency-wide program to manage information security risks. The current agency risk management strategy is ad-hoc, and only focuses on the management of risks at the information system level.

Since the Peace Corps does not foster a risk-based culture, many information systems have been introduced to the network without having the proper security assessments and approvals. The agency has disregarded its responsibility to protect its most sensitive data by introducing an electronic health records system without following the appropriate security assessment and authorization process.

The agency has repeatedly failed to identify all the information systems that operate in the Peace Corps environment. Senior managers have fostered a culture where individual offices are able or allowed to circumvent security controls and introduce unvetted systems to the network.

Without a robust risk management process, the Peace Corps is exposed to attacks, environmental disruptions, or business failures due to human error. Further, the absence of a risk-based culture prevents the agency from making informed decisions that align with agency priorities. By circumventing controls and introducing new systems without following the appropriate security review process, the agency risks leaving the network and its sensitive data vulnerable to exploitation.

EXECUTIVE SUMMARY

BACKGROUND

The Federal Information Security Modernization Act of 2014 (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. 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 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 the Department of Homeland Security.

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) 2016.[1] For more information on the methodology used see Appendix A.

RESULTS IN BRIEF

Our results demonstrate that the Peace Corps lacks an effective information security program because of problems related to people, processes, technology, and culture. Furthermore, OIG found weaknesses across all of the FISMA reportable areas. There are several FISMA findings that have been outstanding for over seven years and the agency has struggled to implement corrective actions.

OIG is concerned about the quality of the IT security program, especially considering the sensitive data that the Peace Corps maintains, such as health records and sexual assault incident information about Peace Corps Volunteers.

Without a comprehensive, integrated IT security program, sensitive agency systems and data are vulnerable to exploitation and failure.

[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.

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 5,000 full-time and part-time personnel distributed throughout the world. The OCIO's IT services affect both domestic Peace Corps staff—located at the Washington, D.C. Headquarters, seven Regional Recruiting Offices, and remote locations connecting via the Virtual Private Network —and international staff located at the Peace Corps' 61 posts worldwide.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Through the Federal Information Security Management Act of 2002,[2] as amended by the Federal Information Security Modernization Act of 2014,[3] Congress recognized the importance of information security to the economic and national security interests of the United States. 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 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 to federal agencies, the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Department of Homeland Security (DHS) in order to strengthen information system security. 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.

[2] 44 U.S.C. §§ 3501-58.

[3] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

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

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 2016.[5] For more information on the methodology used see Appendix A. For a list of federal requirements used as criteria, see Appendix D.

[4] OMB Memorandum M-14-04, Nov. 2013.

[5] 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.

RESULTS

OVERVIEW

Since 2009, the Peace Corps Office of Inspector General (OIG) has reported in its 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 seven years and the agency has struggled to implement corrective actions.

While the agency has dedicated more resources to IT security in the last year and a half, OIG remains concerned about the quality of the IT security program, especially considering the sensitive data that the Peace Corps maintains. Some of the most sensitive data the agency generates and possesses are health records and sexual assault incident information about Peace Corps Volunteers.

Our aggregated results demonstrate that the Peace Corps lacks an effective information security program. We found problems relating to people, processes, technology, and culture. Furthermore, OIG found weaknesses across all the FISMA reportable areas. The following sections are organized around the five information security functions outlined in the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover.

IDENTIFY

Introduction

The agency must identify and develop an understanding of cybersecurity risk that it faces as a whole. To integrate this risk management process throughout the Peace Corps and to address the agency's mission and business concerns, a three-tiered approach—entity, business process, and system—should be employed. The process should be carried out across the three tiers with the objective of continuous improvement in the agency's risk-related activities, with effective communication among tiers and stakeholders.

The entity level addresses risk from an organizational perspective with the development of a comprehensive governance structure and agency-wide risk management strategy. The business process level assesses risk associated with the organizational structure of the agency, and is guided by the risk decisions at the entity level. The system level looks at needed safeguards and countermeasures for agency information systems.

Risk Management

Explicit, well-informed risk-based decisions are crucial in order to balance the benefits of using information systems against the risk of those same information systems being the channels through which attacks, environmental disruptions, or human errors cause business failures. To

effectively manage information security risks, senior executives must be committed to making effective risk management a fundamental business requirement.

Information security risk management must be a holistic activity that involves the entire agency. Organizational culture becomes a key factor in determining how risk is managed within the agency because all individuals are directly influenced by the risk framework established by senior executives. Senior executives both directly and indirectly set the tone for how the agency responds to various approaches to managing risk.

Contractor Systems
In conjunction with understanding the risk environment, the agency must assess and understand the relationship it has with third parties that store agency information and data. There must be adequate controls in place to ensure that information systems operated by contractors and other external entities on behalf of the Peace Corps meet all applicable security requirements.

Areas of Concern

Risk Management
The Peace Corps does not have a robust agency-wide program to manage information security risks. The current agency risk management strategy only focuses on managing the information security risks at the information system level in an ad-hoc manner. Furthermore, their approach overlooks the risks that can potentially impact the agency at the critical business processes and entity levels.

Since the Peace Corps does not facilitate a risk-based culture, many information systems have been introduced to the network without having the proper security assessments and approvals. The agency has disregarded its responsibility to protect its most sensitive data by introducing an electronic health record system without following the appropriate security assessment and authorization process.

The agency has repeatedly failed to identify all the information systems that operate in the Peace Corps environment. Specifically, senior managers have fostered a culture where individual offices are able or allowed to circumvent security controls and introduce unvetted systems to the network.

Contractor Systems
The Peace Corps does not have a thorough understanding of the external system connections that it maintains. This issue stems from inadequate policies and guidance on how to ensure third party system compliance with federal cybersecurity requirements. Furthermore, the Peace Corps is unable to demonstrate it exercised due diligence in reviewing external entity system controls because there is no documentation of agency actions taken.

Agency Response

The agency concurred with the two findings in this area and plans to take action to address the areas of concern identified.

Impact

Because it has not effectively realized a robust risk management process at the entity level, the Peace Corps may be incapable of addressing the root causes associated with existing information security risks. Such an imbalance may invariably expose the Peace Corps to attacks, environmental disruptions, or business failures due to human error. Further, the absence of a risk-based culture could prevent the agency from making well-informed decisions to ensure that the results align with agency priorities. By circumventing controls and introducing new systems without following the appropriate security review process, the agency risks leaving the network and its sensitive data vulnerable to exploitation.

Additionally, without adequate oversight of external systems, there is minimal assurance that third party systems' information security controls maintain compliance with federal standards. This could cause security lapses, leading to unauthorized users having the ability to exploit the systems and access the Peace Corps' sensitive data.

PROTECT

Introduction

The agency must develop and implement appropriate safeguards to ensure that information systems are protected, and users of those systems are appropriately vetted and trained.

Configuration Management
Configuration management is composed of activities that ensure the integrity of information systems and prevent negative impacts to overall information security or system functionality. Information systems are constantly changing in response to updated hardware or software capabilities, and patches for correcting software flaws. The implementation of such changes usually results in some adjustment to the system configuration. Therefore, a well-defined configuration management process must consider information security when determining how to implement the necessary adjustments.

Identity and Access Management
Users and devices must be validated to ensure that they are who or what they identify themselves to be. The purpose of identity and access management is to ensure that only properly authorized users and devices have access to information and information systems.

Security and Privacy Training
Establishing and maintaining a comprehensive information security training process provides all users with the information and tools needed to protect systems and sensitive data. This will

ensure that personnel at all levels of the agency understand their information security responsibilities to properly use and protect the information and resources entrusted to them.

Areas of Concern

Configuration Management
The Peace Corps does not have the fundamental components of a configuration management program. Specifically, it has not consistently implemented policies and procedures in making changes to its information systems. Furthermore, the agency lacks a centralized technology solution to effectively track and monitor software and hardware inventories to ensure configurations are properly maintained. In addition, for multiple months, the agency failed to install critical software patches at headquarters, regional recruiting offices, and posts.

Identity and Access Management
The Peace Corps has not consistently implemented user access management processes at the entity and system levels. While the Peace Corps has developed a clear process for granting users access, the implementation of this process has been inconsistent. Furthermore, despite federal requirements mandating multi-factor authentication by FY 2012, the Peace Corps has yet to abide by these federal requirements.

Security and Privacy Training
The Peace Corps has made progress in enhancing its security awareness training program by providing some formal training to users with privileged access to the network. However, the agency definition of who should receive this additional formal training is not inclusive of users with significant influence on decision-making, program oversight, and entity level security posture.

Agency Response

The agency concurred with 5 of the 6 findings in this area and plans to take action to address the areas of concern identified. For the finding that the agency did not concur with, the Peace Corps believes corrective actions had already been taken to resolve the issue; however OIG did not identify sufficient corrective actions to consider this noncompliance resolved. Therefore the finding remains open.

Impact

The absence of a comprehensive configuration management program hinders the Peace Corps' ability to provide adequate information security. Additionally, the agency's risk management process is compromised by improperly implemented agency policies and inaccurate hardware and software inventories. Consequently, the risk for data loss, data manipulation, and system unavailability is increased.

Without effective identity and access management, the risk of unauthorized access is significantly increased. Unauthorized access may result in the dissemination of sensitive data and other malicious activities.

Without the completion of proper security training, Peace Corps staff may be unaware of new risks that may compromise the confidentiality, integrity, and availability of data. Furthermore, this lack of understanding has resulted in Peace Corps staff circumventing security controls over the agency's most sensitive data. This could result in a temporary loss of operations, inappropriate dissemination of sensitive information, and the introduction of vulnerabilities to the system.

DETECT

Introduction

The Peace Corps' mission-critical functions depend upon information technology. Therefore, its ability to manage this technology and assure the confidentiality, integrity, and availability of information is mission-critical. Additionally, as the Peace Corps' ability to make timely organizational risk management decisions is partially contingent upon maintaining awareness of information security, vulnerabilities, and threats, the agency must be able to discover and identify cybersecurity events in real-time.

Continuous Monitoring
Continuous monitoring is the process of maintaining ongoing awareness of information security vulnerabilities, threats, and the effectiveness of deployed security controls. This program aids senior executives in making organizational and information system risk management decisions that cost-effectively align with IT security objectives and goals.

Areas of Concern

The Peace Corps has not fully implemented a continuous monitoring program at the information system level. Specifically, activities are performed in an ad-hoc and reactive manner. The agency also lacks defined security metrics to monitor information security risks in real-time. Furthermore, the agency has not defined how it integrates continuous monitoring activities above the information system level.

Agency Response

The agency concurred with the finding in this area and plans to take action to address the areas of concern identified.

Impact

The lack of a comprehensive continuous monitoring program prevents the Peace Corps from gauging the security posture of its information systems at any given time. It also prevents the agency from effectively monitoring a dynamic IT environment with changing threats, vulnerabilities, technologies, business functions, and critical missions. Without a fully implemented continuous monitoring program, potential damage to agency systems could occur, which may result in system downtime, unauthorized access, changes to data, data loss, or operational failure.

RESPOND

Introduction

The Peace Corps must be able to take appropriate action regarding a cybersecurity event, as attacks frequently compromise personal and business data. Preventive activities based on risk assessments can lower the number of incidents, but not all incidents can be prevented. It is critical the agency respond quickly and effectively when security breaches do occur.

Incident Response
An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring information technology services. The purpose of incident response and reporting is to determine the types of attacks that have been successful and position the agency to make a risk-based decision about where it is most cost effective to focus its security resources.

Areas of Concern

The Peace Corps has been making ongoing progress towards implementing an effective incident response and reporting program. In the last year, the Peace Corps designated a full time incident response specialist and updated its incident response plan. However, this plan lacks a process for maturing and strengthening the incident response program as required by federal standards. Furthermore, while the Peace Corps has introduced some automated tools, these have not been fully leveraged for timely identification of risk.

Agency Response

The agency concurred with the finding in this area and plans to take action to address the areas of concern identified.

Impact

Without a strong incident response program, sensitive agency systems and data are vulnerable to exploitation. Lacking a process to mature the incident response plan prevents the agency from responding to evolving and sophisticated threats in a near real-time manner. Furthermore, without efficient threat monitoring and mitigation, there is a higher risk for attacks on

information systems and extended system outages inhibiting staff from conducting essential business functions.

RECOVER

Introduction

Information systems are critical to the Peace Corps' mission. The agency must develop and implement a strategy to ensure that these systems are able to operate effectively without excessive downtime.

Contingency Planning
Contingency planning supports this concept by establishing thorough plans, procedures, and technical measures that allow systems to be recovered as quickly and effectively as possible following a cybersecurity event. The primary purpose of contingency planning is to give attention to events that have the potential for significant consequences and prioritize the restoration of mission-critical systems.

Areas of Concern

While the Peace Corps has worked to formalize contingency planning at the entity, business process, and system levels, its approach has not been integrated. Specifically, the information at each level has not been developed in coordination with the mission and business processes that they support. In addition, there has been a lack of coordination between responsible parties to ensure the independent plans support a unified agency response to a disruption.

Agency Response

The agency did not concur with the finding in this area. The Peace Corps' response to OIG indicated that they do not understand the relationship between entity level contingency planning and system level contingency planning. The agency's failure to recognize the relationship between these types of contingency plans, established by federal standards, impedes the agency from protecting critical assets from extended down periods.

Impact

Without effective contingency plans, the agency may be unable to prioritize its resources to restore and recover mission-critical business functions in the event of a disaster. Furthermore, a lack of coordination at the entity, business process, and system level is not cost effective in addressing contingency planning concerns.

APPENDIX A: SCOPE AND METHODOLOGY

FISMA, as amended by the Federal Information Security Modernization Act of 2014, 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 2016 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 2016.

The Peace Corps OIG contracted accounting and management consulting firm Williams, Adley & Company-DC to perform the assessment of the Peace Corps' compliance with the provisions of FISMA. Williams Adley performed this review from May to September 2016. They performed the review in accordance with *Generally Accepted Government Auditing Standards* (GAGAS), FISMA, OMB, and NIST guidance. GAGAS requires that Williams Adley plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the review objectives. 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:

- OMB Memorandums M-02-01 Guidance for Preparing and Submitting Security Plans of Action and Milestones, M-04-04 E-Authentication Guidance for Federal Agencies, M-06-19 Reporting Incidents Involving Personally Identifiable information and Incorporation the Cost for Security in Agency Information Technology Investments, and M-14-04 FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

- The Peace Corps' policies and procedures

- Federal laws, regulations, and standards such as FISMA, OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources and OMB Circular No. A-11

- NIST publications, Federal Information Processing Standards, and industry best practices.

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

DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
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

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. NIST SP 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*
      v. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Security Systems*
   b. Contractor Systems
      i. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

II. Protect
   a. Configuration Management
      i. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
   b. Identity and Access Management
      i. HSPD-12, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors
      ii. OMB M-11-11
      iii. OMB M-04-04
   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*
      iii. NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*

IV. Respond
    a. Incident Response
        i. NIST SP 800-61 Revision 1, *Contingency Planning Guide for Federal Information Systems*
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*

Help Promote the Integrity, Efficiency, and Effectiveness of the Peace Corps

Anyone knowing of wasteful practices, abuse, mismanagement, fraud, or unlawful activity involving Peace Corps programs or personnel should contact the Office of Inspector General. Reports or complaints can also be made anonymously.

Contact OIG

Reporting Hotline:

U.S./International:	202.692.2915
Toll-Free (U.S. only):	800.233.5874
Email:	**OIG@peacecorps.gov**
Online Reporting Tool:	**peacecorps.gov/OIG/ContactOIG**
Mail:	Peace Corps Office of Inspector General P.O. Box 57129 Washington, DC 20037-7129

For General Information:

Main Office:	202.692.2900
Website:	**peacecorps.gov/OIG**
Twitter:	**twitter.com/PCOIG**