PEACE CORPS
Office of
INSPECTOR GENERAL

Our Mission:

Through audits, evaluations, and investigations, the Office of Inspector General provides independent oversight of agency programs and operations in support of the goals set forth in the Peace Corps Act while making the best use of taxpayer dollars.

Report on the Peace Corps' Information Security Program

FISCAL YEAR 2017

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 (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. 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 FY 2017.[1]

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, the Office of Inspector General (OIG) found weaknesses across all of the FISMA reportable areas. There are several FISMA findings that have been outstanding for over 7 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.

To ensure the agency's information, operations, and assets are protected, it is critical that the Peace Corps achieve full compliance with FISMA and other Federal laws and regulations that apply to managing its IT security infrastructure. The Peace Corps needs to embrace a risk-based culture and place greater emphasis on the importance of a robust information security program by involving senior leadership, ensuring agency policies are comprehensive, and prioritizing the time and resources necessary to become fully FISMA compliant and eliminate weaknesses.

[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.

Contact

Have questions? Need to talk to us?

Hotline

Confidentially report fraud, waste, abuse, or mismanagement in the Peace Corps.

Online: www.peacecorps.gov/OIG/

Email: OIG@peacecorpsoig.gov

Phone: (202) 692-2915

Mail: Peace Corps
Office of Inspector General
P.O. Box 57129
Washington, DC 20037-7129

General Information

Talk to OIG staff about general business.

Online: www.peacecorps.gov/OIG

Twitter: @PCOIG

Phone: (202) 692-2900

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. OCIO's IT services affect both domestic Peace Corps staff—located at the Washington, D.C. headquarters, six regional recruiting offices, and remote locations connected 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 (FISMA),[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 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

[2] Pub. L. No. 107-347, 116 Stat. 2899, 2947 (Dec. 17, 2012), codified in relevant part at 44 U.S.C. §§ 3501-58.

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

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.[4] OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

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.

- **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.

Each of these function areas, as it relates to the Peace Corps, will be discussed in the below "Results" section of the report.

Maturity Model

The fiscal year (FY) 2017 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 2017 IG FISMA Metrics provide maturity models for all five security functions and reorganize the models—provided in

[4] E.g., OMB Memorandum M-17-05, Nov. 2016.

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 2017.[5] For more information on the methodology used, see Appendix A. For a list of Federal requirements used as criteria, see Appendix D.

[5] The Peace Corps Office of Inspector General contracted accounting and management consulting firm Williams, Adley & Company-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 7 years and the agency has struggled to implement corrective actions.

While the agency has dedicated more resources to the IT security program in the last 2 years, OIG remains concerned about the agency's approach to IT security, especially considering the sensitive data that the Peace Corps maintains about Peace Corps Volunteers, specifically records related to health, medical treatment, and crime incidents including information on sexual assault cases. Peace Corps senior leadership has not been sufficiently involved in IT security and has not fostered a risk-based culture. OCIO has made improvements to information security at the information system level; however, involvement from all levels of Peace Corps leadership is needed to advance and fully develop the agency's information security program.

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. Based on assessments against the FY 2017 FISMA Metrics, each function area has been rated with a maturity level.

IDENTIFY

Introduction

The activities in the "identify" function are foundational for effective use of the Cybersecurity Framework. An organization that understands its business context, the resources that support critical functions, and the related information security risks can focus and prioritize its efforts consistent with its risk management strategy and business needs.

Therefore, the agency must identify and develop an understanding of the cybersecurity risk that it faces as a whole. A three-tiered approach—entity, business process, and system—should be employed to integrate this risk management process throughout the Peace Corps and to address the agency's mission and business concerns. 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 through 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 leadership 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 staff. Senior staff 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 as the agency does not have an organization-wide information security risk management strategy. The current agency risk management strategy only focuses on managing the information security risks at the information system level in an ad-hoc manner, overlooking the risks that can potentially impact the agency at the critical business processes and entity levels, including in processes related to finances, physical security, information security, and property management. Furthermore, the risk management strategy has not defined the agency's information security risk profile, risk appetite, risk tolerance, and process for communicating risks to all necessary internal and external stakeholders. In addition, the lack of senior management involvement in framing risk hinders the Peace Corps' ability to effectively make organization-wide risk management decisions that guide risk management activities carried out by all stakeholders.

Moreover, 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 routinely circumvent security controls and introduce unvetted systems to the network.

Contractor Systems
The Peace Corps does not have comprehensive policies and procedures for overseeing contractor system information security to ensure third party systems comply with Federal cybersecurity

requirements. Accordingly, the Peace Corps is unable to demonstrate effective maintenance of system interconnection documentation.

Maturity Level

In summary, the agency has only achieved level 1, ad-hoc maturity rating, for this function area.

Agency Response

Concur. Since establishing risk management as an objective in its 2018-2022 strategic plan, Peace Corps is developing an enterprise risk management strategy that considers risks at the entity, business unit and information system levels. A central tenet of this strategy will be the integration and consideration of cybersecurity, physical, financial, personnel and privacy to proactively address risks and opportunities, develop strategies and monitor progress. The agency is also in the process of improving information security policy and procedures to address deficiencies in System Assessment and Authorization as well as Contractor System oversight.

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. A weak risk management process 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.

Recommendations

Risk Management

1. OIG recommends that the Peace Corps Director and Agency Risk Executive, in coordination with Peace Corps senior leadership, identify the agency's information security risk profile, and define the agency's risk appetite and risk tolerance.

2. OIG recommends that the Agency Risk Executive, in coordination with Peace Corps senior leadership, develop and implement an enterprise-wide risk management strategy to address how to identify, assess, respond to, and monitor security-related risks in a holistic approach across the organization, business process, and information system levels.

3. OIG recommends that Office of the Chief Information Officer perform all components of the Security Assessment and Authorization on all FISMA reportable systems in accordance with the risk management strategy.

4. OIG recommends that Office of the Chief Information Officer develop an information security architecture that is integrated with the risk management strategy.

5. OIG recommends that the Office of the Chief Information Officer develop and implement procedures for performing e-authentication risk assessments on systems according to Office of Management and Budget Memorandum M-04-04 guidelines.

Contractor Systems

6. OIG recommends that the Office of the Chief Information Officer, in coordination with Acquisitions and Contracts Management, update and implement contract oversight policies and procedures to include information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information.

PROTECT

Introduction

The “protect” function of the Cybersecurity Framework supports the ability to limit or contain the impact of a potential information security event. As such, 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 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 developed, maintained, or implemented a comprehensive enterprise-wide configuration management plan. Furthermore, the agency lacks policies and procedures to track and monitor software and hardware inventories to ensure configurations are properly implemented and maintained. In addition, the agency failed to install critical software patches at posts.

Identity and Access Management

The Peace Corps has not consistently implemented user access management processes at the entity and system levels. While the agency has developed a clear process for granting users access, the implementation of this process has been inconsistent. Although multi-factor authentication has been partially implemented at headquarters for logical access, the Peace Corps has yet to fully abide by Federal requirements mandating multi-factor authentication. In addition, the agency has not defined an Identity, Credential, Access Management Strategy to align with the architecture and guidance provided in the Federal, Identity, Credential, Access Management Roadmap and Guidance.

Security Training

The Peace Corps improved its security awareness training program by identifying personnel with significant security responsibilities and providing them with more tailored course offerings. However, the current program has not been developed to consider risk designations based on security roles and responsibilities when identifying users requiring role-based security training.

Maturity Level

In summary, the agency has only achieved a level 1, ad-hoc maturity rating, for this function area.

Agency Response

Concur. Peace Corps is currently in the process of revising its information security policies and processes to address the noted gaps in configuration management, identity credentialing and management and security awareness training. It should also be noted that Trusted Internet Connection, in coordination with improvements to its data center, is scheduled for deployment this fiscal year.

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.

The agency's ineffective identity and access management significantly increases the risk of unauthorized access. 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.

Recommendations

Configuration Management

7. OIG recommends that the Office of the Chief Information Officer develop a comprehensive enterprise-wide configuration management plan.

8. OIG recommends that the Office of the Chief Information Officer develop policies and procedures for maintaining up-to-date inventory of software and hardware assets.

9. OIG recommends that the Office of the Chief Information Officer implement, monitor, and maintain up-to-date patches and authorized software to manage its information technology assets supporting all FISMA reportable systems in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4 requirements.

10. OIG recommends that the Office of the Chief Information Officer implement a trusted internet connection to reduce and consolidate external connections.

Identity and Access Management

11. OIG recommends that the Office of the Chief Information Officer develop and implement an Identity Credential and Access management strategy to manage user access.

12. OIG recommends that the Office of the Chief Information Officer develop a process to track when new user accounts are created and activated to ensure that activation does not occur prior to the hire date.

13. OIG recommends that the Office of the Chief Information Officer develop a process to identify and track all privileged users at the information system level to ensure the rules of behavior and appropriate security training have been provided timely.

14. OIG recommends that the Office of Chief Information Officer use risk designations, based on security roles and responsibilities, when tailoring and developing security training course offerings.

15. OIG recommends that Office of the Chief Information Officer fully implement Personal Identity Verification cards to gain logical access to the Peace Corps' information systems as required by Homeland Security Presidential Directive-12.

16. OIG recommends that Office of Safety and Security implement Personal Identity Verification cards to gain physical access to the Peace Corps' domestic facilities as required by Homeland Security Presidential Directive-12.

DETECT

Introduction

The "detect" function of the Cybersecurity Framework enables timely discovery of an information security event. The Peace Corps' mission-critical functions depend upon information technology, and so 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 staff 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 does not have a defined information security continuous monitoring (ISCM) strategy with supporting policies and procedures. Furthermore, the Peace Corps has not defined key security metrics specifically to measure the effectiveness of its ISCM program.

Maturity Level

In summary, the agency has only achieved a level 1, ad-hoc maturity rating, for this function area.

Agency Response

Concur. Although the agency collects and reports key metrics, the application of those metrics has not been codified into policy or procedure. Peace Corps is currently in the process of revising its information security policies and processes to strengthen its information system continuous monitoring (ISCM) program.

Impact

The Peace Corps’ lack of a comprehensive continuous monitoring program prevents it 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.

Recommendations

17. OIG recommends that the Office of the Chief Information Officer develop and fully implement an Information Security Continuous Monitoring strategy that includes policies and procedures; defined roles and responsibilities; and security metrics to measure effectiveness.

RESPOND

Introduction

The “respond” function of the Cybersecurity Framework supports the ability to contain the impact of a potential information security event.

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

Although the Peace Corps has been making efforts to implement an effective incident response program, the agency did not revise the Incident Response Plan to include updated Federal reporting requirements. In addition, the Incident Response Team did not prioritize testing of incident response capabilities which allow for consistent implementation of incident response policies and procedures.

Maturity Level

In summary, the agency has only achieved a level 2, defined maturity rating, for this function area.

Agency Response

Concur. The Incident Response program has been updated to reflect current US-CERT reporting standards.

Impact

Without a strong incident response program, sensitive agency systems and data are vulnerable to exploitation. The agency's lack of a process to mature the incident response plan prevents it 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.

Recommendations

18. OIG recommends that the Office of the Chief Information Officer update the Information Response Plan to include maturation plans and ensure alignment with Federal reporting standards.

RECOVER

Introduction

The "recover" function of the Cybersecurity Framework supports timely recovery to normal operations to reduce the impact from an information security event. As 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

The Peace Corps lacks a process to coordinate changes between the Continuity of Operations Plan, Disaster Recovery Plan, and all information system contingency plans to ensure the respective plans support a unified agency response to a disruption. In addition, the agency has not demonstrated efforts to maintain the existing disaster recovery process given its plan to move the disaster recovery functionality to a cloud-based system.

Maturity Level

In summary, the agency has only achieved a level 1, ad-hoc maturity rating, for this function area.

Agency Response

Concur. Peace Corps is currently in the process of revising its information security policies and processes to formalize coordination of changes to Continuity of Operations, Disaster Recovery and Contingency Planning.

Impact

Without effective contingency program, 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.

Recommendations

19. OIG recommends that the Office of the Chief Information Officer, in coordination with the Office of Safety and Security, develop a process to coordinate changes between the Continuity of Operations Plan, Disaster Recovery Plan, and all information system contingency plans to ensure that the plans align.

20. OIG recommends that the Office of the Chief Information Officer update the Disaster Recovery Plan.

CONCLUSION

Overall, the agency has been assessed at a level 1, ad-hoc maturity rating. Since level 4, managed and measurable, is considered to be an effective level of security, the Peace Corps requires extensive effort to achieve a robust and effective information security program.

To ensure the agency’s information, operations, and assets are protected, it is critical that the Peace Corps achieve full compliance with FISMA and other Federal laws and regulations that apply to managing its IT security infrastructure. The Peace Corps needs to embrace a risk-based culture and place greater emphasis on the importance of a robust information security program by involving senior leadership, ensuring agency policies are comprehensive, and prioritizing the time and resources necessary to become fully FISMA compliant and eliminate weaknesses.

Focusing on the implementation of the Risk Management Framework will facilitate the tailoring of an information security program that meets the Peace Corps' mission and business needs across a decentralized organization.

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 2017 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 2017:

- Donate.Peacecorps.gov,
- Medical Applicant Exchange (MAXx),
- Peace Corps Medical Electronic Documentation and Inventory Control System (PCMEDICS), and
- Safety and Security.

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 2017. 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:

- FY 2017 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-17-05 "Fiscal Year 2016-2017 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

DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
ISCM	Information Security Continuous Monitoring
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*
      vi. OMB M-04-04
   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 800-128, *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*
      iii. OMB M-09-32
   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*