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

Background

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

This is a summary of the results of that review.

What OIG Reviewed

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 2015 complied with applicable Federal laws, regulations, and information security standards.

Review of Peace Corps' Information Security Program

November 2015

What We Found

We identified control weaknesses that significantly impacted Peace Corps' information security program. While Peace Corps had made small adjustments to improve its information security program in FY 2015, we continued to find similar non-compliance with Federal laws, regulations, and information security standards that we have seen in our reviews since FY 2013. Specifically, we identified control deficiencies in nine of the 10 information security program areas.

Peace Corps did not meet the following specific security requirements:

1. developing and implementing an organization-wide risk management strategy at all levels of the organization;
2. implementing an enterprise-wide continuous monitoring strategy to include the continuous monitoring program metric;
3. implementing Personally Identity Verification authentication at headquarters, posts, and regional recruiting offices for both physical and logical access;
4. effectively managing user accounts; and
5. clearly identifying and managing system inventories to implement configuration management for all its systems.

In addition, we have identified other information security program areas that need significant improvements, including contingency planning, incident response and reporting, security training, remote access, and contractor oversight.

Collectively, the control deficiencies we identified during this review represent a significant deficiency to enterprise-wide security, as defined by OMB Memorandum M-14-04. As a result, these deficiencies place critical information systems and sensitive data used to support the agency's operations, assets, and key personnel at risk, and can potentially impair the agency's efforts to fully implement effective information security programs. Furthermore, a potential security breach could compromise the security of the network, resulting in a loss of information; compromise of Personally Identifiable Information; denial of service attacks; damage to the general support systems; improper access; dissemination of confidential data; and the introduction of vulnerabilities to all of Peace Corps' systems.

What We Recommended

OIG made 18 recommendations to improve Peace Corps' information security program. The most significant of which are that Peace Corps:

1. fully develop and implement an organization-wide risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization; and
2. develop and adhere to a formal project plan to assign the proper resources required to fully implement all components of its current information security continuous monitoring strategy.