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

# Report on Protecting Sensitive Information in Peace Corps Computer Systems

August 2016

## Background

The Consolidated Appropriations Act of 2016 required Offices of Inspectors General (OIGs) to provide Congress with a report describing controls used by their agencies to protect sensitive information maintained, processed, and transmitted by agency computer systems.

## What We Did

The Peace Corps identified 12 systems in its current production environment that contain sensitive information. OIG contracted with accounting and management consulting firm Williams, Adley & Company-DC to perform the review of these systems. Williams Adley selected four of those 12 systems to review using a risk based approach.

Williams Adley performed the review from May 2016 to July 2016. They interviewed Peace Corps officials to gain an understanding of the agency's current information security policies and procedures related to the Peace Corps' computer security controls for the systems. Williams Adley also collected and reviewed relevant written documents related to four Personally Identifying Information systems we selected. The documents reviewed included system security plans and relevant Peace Corps Manual sections.

## What We Found

While the Peace Corps had dedicated more resources to IT security in the last year and a half, we remain concerned about the quality of the IT security program, especially considering the sensitive data that the agency maintained. The agency not only generated and possessed standard personally identifiable information, but also maintained health records and sexual assault incident information about Peace Corps Volunteers. The lack of controls related to sensitive information, including the use of multi-factor authentication, undermines IT security.

Overall, the Peace Corps had in place overarching logical access policies and practices. However, we found that the access control policies for two out of four systems we reviewed did not consistently follow federal information security guidance and standards. Furthermore, the Peace Corps did not have formal policies or procedures for managing software inventories. The Peace Corps reported having limited exfiltration capabilities, utilizing some tools to help with forensics and network visibility.

The Peace Corps had developed information security policies and procedures for managing contracted and hosted information systems. Based on an OIG recommendation, the agency implemented policies to review IT security as a key part of acquisition when pursuing cloud services. However, since 2013 there has been an outstanding Federal Information Security Management Act (FISMA) finding that the agency has not adequately tracked or monitored contract agreements and memorandums of understanding in its official security repository.

Our report noted that the statements regarding the Peace Corps system security environment were provided by officials from the Office of the Chief Information Officer and have not been verified through testing. This testing will occur as part of the 2016 annual FISMA review, which will be summarized in the next Semiannual Report to Congress.