OFFICE OF INSPECTOR GENERAL

AUDIT OF USAID'S FISCAL YEAR 2014 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

AUDIT REPORT NO. A-000-15-003-P
October 30, 2014

WASHINGTON, DC

This is a summary of our report on the "Audit of USAID's Fiscal Year 2014 Compliance With the Federal Information Security Management Act of 2002." Referred to as FISMA, the act requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. FISMA also requires agencies to have an annual assessment of their information systems.

The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Cotton & Company LLP to conduct the audit. Cotton was required to conduct the audit in accordance with U.S. Government auditing standards. The objective was to determine whether USAID implemented selected minimum security controls for selected information systems in support of FISMA.

The audit concluded that USAID does not comply with FISMA. Although the Agency has developed and documented the majority of the information security policies and procedures required under the act, USAID has not established an effective risk management program to ensure that policies and procedures are assessed and working as intended. Consequently, the audit found a number of information system weaknesses that, if exploited, could adversely affect the confidentiality, integrity, and availability of USAID's data and information systems, and ultimately could have a negative impact on the Agency's ability to protect the security of its information or information systems.

OIG made 18 recommendations to address the weaknesses identified and to help USAID strengthen its information security program. Management decisions were made on all of them.