OFFICE OF INSPECTOR GENERAL

AUDIT OF USAID'S IMPLEMENTATION OF KEY COMPONENTS OF A PRIVACY PROGRAM FOR ITS INFORMATION TECHNOLOGY SYSTEMS

AUDIT REPORT NO. A-000-15-001-P
OCTOBER 10, 2014

WASHINGTON, DC

This is a summary of our report on the *Audit of USAID's Implementation of Key Components of a Privacy Program for Its Information Technology Systems*.

The Privacy Act of 1974, as amended, defines the rights and responsibilities for maintaining, protecting, and disclosing personal information. The act requires that agencies:

- Publish notices describing systems of records.

- Make reasonable efforts to maintain accurate, relevant, timely, and complete records about individuals.

- Manage those records in a way to ensure fairness to individuals in agency programs.

The U.S. Congress and Office of Management and Budget (OMB) have instituted a number of laws and regulations that govern protection of individuals' privacy. OMB issued Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (September 26, 2003), which requires federal agencies to (1) conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available, and (2) post privacy policies on agencies' public Web sites.

OIG conducted this audit to determine whether USAID implemented key components of a privacy program for its information technology systems to mitigate the risk of violations against key privacy requirements. For this audit, "key components" of a privacy program are (1) privacy management structure, including clear assignment of roles and responsibilities, (2) policies and procedures, (3) awareness and training, and (4) monitoring for compliance.

The audit found that USAID did not implement these key components because it did not do the following:

- Designate a senior agency official for privacy. Therefore, the Agency did not have a senior-level individual who is responsible for making sure it complies with privacy laws, regulations, and policies.

- Fully provide basic privacy training. Thus, employees may not know how to handle personally identifiable information (PII), which puts the Agency at risk of privacy breaches and incidents.

- Fully provide role-based privacy training. Employees who handle PII regularly may not have the knowledge and skills needed to protect the information and therefore are at risk of causing a breach.

- Complete system of records notices for three of four judgmentally selected systems. People do not have an opportunity to review their records for accuracy if they do not know the system of records exists. Further, any officer or employee who willfully maintains a system of records without meeting the Privacy Act of 1974, as amended, is guilty of a misdemeanor and may be fined up to $5,000.

- Complete privacy impact assessments for its third-party Web sites. Thus, USAID did not make sure that it collected information in conformance with applicable legal, regulatory, and policy requirements.

- Post privacy notices for six judgmentally selected third-party Web sites that made PII available to the Agency. People may not understand the potential impact on their privacy when they use third-party Web sites that make their PII available to the Agency.

- Address all requirements in the Agency's privacy breach notification procedures. Therefore, USAID's Breach Response Team may not fully understand how to handle a privacy breach.

- Provide working links on the Agency's external Web site to system of record notices and the privacy impact assessment for AIDNet, the Agency's computer network. Thus, the public may not be aware of what PII the Agency is collecting or how the Agency collects, uses, and stores PII in AIDNet.

- Update its electronic records disposition schedule. As a result, USAID cannot be sure that Agency officials know when to dispose of electronic records that contain PII.

- Require in its privacy impact assessment procedures that the assessments address how people can consent to provide information for particular uses. Members of the public may not have been fully aware that certain actions they take may imply their consent.

Although some of these weaknesses have other attributing causes, most of them can be attributed to the following three; USAID (1) did not make its privacy program a priority within the organization, (2) had a material weakness[1] due to its decentralized information technology security program, and (3) allocated a questionable level of resources to the program.

To address the weaknesses, this report contains 34 recommendations to help USAID strengthen its privacy program. Based on our evaluation of USAID's management comments and other communications, we acknowledge management decisions on all 34 and final action on 7.

[1] OMB Circular A-123, "Management's Responsibility for Internal Control" (December 21, 2004) defines a material weakness as a control deficiency that the agency head determines to be significant enough to report outside of the agency.

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
http://oig.usaid.gov