USAID
FROM THE AMERICAN PEOPLE

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-000-06-003-P
June 8, 2006

WASHINGTON, DC

Office of Inspector General

June 8, 2006

MEMORANDUM

TO: A-AA/M, Mosina Jordan
AA/LPA, J. Edward Fox

FROM: AIG/A, Joseph Farinella /s/

SUBJECT: Audit of USAID's Implementation of Key Components of a Privacy Program for its Information Technology Systems (Report No. A-000-06-003-P)

This memorandum transmits our final report on the subject audit. We have considered your comments on the draft report and have included your response (excluding the attachment) in its entirety in Appendix II.

This report contains nine recommendations to help USAID improve its privacy program over its information technology systems. Based on your response and the supporting documentation provided, final action has been taken on Recommendation No. 1. In addition, management decisions have been reached on Recommendation Nos. 2 through 8. Please notify the Bureau for Management's Audit, Performance and Compliance Division when final action is completed.

Again, I want to express my sincere appreciation for the cooperation and courtesies extended to my staff during this audit.

U.S. Agency for International Development
1300 Pennsylvania Avenue, NW
Washington, DC 20523
www.usaid.gov

CONTENTS

SUMMARY OF RESULTS

The Information Technology and Special Audits Division of the Office of Inspector General in Washington, D.C. initiated this audit to address selected privacy reporting requirements outlined in the E-Government Act of 2002 and the Privacy Act of 1974. (See page 2.)

Overall, this audit found that USAID did not implement key components of a privacy program for its information technology systems to mitigate the risk of violations against key information technology privacy requirements. Specifically, USAID did not have a:

- Privacy management structure, including:
  - A key privacy official with full authority over the Agency's privacy program, as required.
  - Other privacy roles and corresponding responsibilities.
- Comprehensive set of privacy policies and procedures, including:
  - Privacy policies and procedures fully referenced to other requirements.
  - Procedures for privacy impact assessments.
  - Procedures for responding to privacy violations.
- Privacy training and awareness program.
- Process to monitor compliance with privacy requirements, including:
  - Updates to and creation of System of Records Notices.
  - Agency-funded websites. (See pages 3-13.)

These weaknesses occurred primarily because USAID officials did not consider privacy to be a high priority and, therefore, did not take actions to correct known weaknesses. (See pages 13-14.) As a result, USAID did not always protect personally identifying information about the public. (See page 13.)

As such, we are making nine recommendations to help USAID develop and implement a privacy program for its information technology systems. (See pages 6-15.)

USAID management agreed to take corrective action on all nine recommendations in the report. Based on your response and the supporting documentation provided, final action has been taken on Recommendation No. 1. In addition, management decisions have been reached on Recommendation Nos. 2 through 8. (See page 16.)

BACKGROUND

The Privacy Act of 1974 was created in response to concerns about the collection and use of personal information, which might impact an individual's privacy rights. The Privacy Act states that each agency that maintains a system of records[1] shall retain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency.

In addition, the E-Government Act of 2002 was signed by the President on December 17, 2002, and became effective on April 17, 2003. The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, privacy policies and practices in the federal agencies will ensure that information is handled in a manner that maximizes privacy.

Section 208 of the E-Government Act of 2002 requires that the Office of Management and Budget (OMB) issue guidance to agencies on implementing the privacy provisions of the E-Government Act. Accordingly, OMB issued Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," dated September 26, 2003. According to the Memorandum, federal agencies are required to, among other things: (1) conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available and (2) post privacy policies on agency websites used by the public.

In order for an Agency to have a viable privacy program, there are several essential elements that must be present: (1) a privacy management structure; (2) policies and procedures, including violation response; (3) awareness and training; and (4) monitoring compliance.

AUDIT OBJECTIVE

This audit was initiated to address selected privacy reporting requirements outlined in the E-Government Act of 2002 and the Privacy Act of 1974. As such, this audit was added to the Office of Inspector General's annual audit plan to answer the following question:

> **Did USAID implement key components of a privacy program for its information technology systems to mitigate the risk of violations against key information technology 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, including violation response; (3) awareness and training; and (4) monitoring compliance.

A description of our scope and methodology is contained in Appendix I.

[1] A system of records is a group of records that maintains personally identifying information about an individual.

AUDIT FINDINGS

USAID did not implement key components of a privacy program for its information technology systems to mitigate the risk of violations against key information technology privacy requirements.

Specifically, USAID did not have a:

- Privacy management structure, including:
  - A key privacy official with authority over the Agency's privacy program, as required.
  - Other privacy roles and corresponding responsibilities.
- Comprehensive set of privacy policies and procedures, including:
  - Privacy policies and procedures fully referenced to other requirements.
  - Procedures for privacy impact assessments.
  - Procedures for responding to privacy violations.
- Privacy training and awareness program.
- Process to monitor compliance with privacy requirements, including:
  - Updates to and creation of System of Records Notices.
  - Agency-funded websites.

The following section discusses this issue in detail.

USAID Did Not Implement Key Components of a Privacy Program

Summary: USAID did not implement key components of a privacy program for its information technology systems to mitigate the risk of violations against key information technology privacy requirements. Specifically, USAID did not have a (1) privacy management structure, (2) comprehensive set of privacy policies and procedures, (3) privacy training and awareness program, and (4) process to monitor compliance with privacy requirements. These weaknesses occurred primarily because USAID officials did not consider privacy to be a high priority and, therefore, did not take actions to correct known weaknesses. As a result, USAID did not always protect personally identifying information about the public.

The following discusses the key components of a privacy program that USAID needs to implement for its information technology systems.

USAID Needs a Privacy Management Structure – According to the U.S. Government Accountability Office's (GAO) "Standards for Internal Control in the Federal Government," one factor affecting the control environment is the agency's organizational structure. Organizational structure provides management's framework for (1) planning, (2) directing; and (3) controlling operations to achieve agency objectives. Thus, a strong internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

However, as discussed in the following sections, USAID did not (1) appoint a key Agency privacy official with authority over the Agency's privacy program, as required, and (2) assign other privacy roles and responsibilities. [See "Cause of Problems Identified" section (pages 13-14) for a discussion of the reason USAID did not have a privacy management structure in place.]

Key Agency Privacy Official Needed – Office of Management and Budget Memorandum (OMB) M-05-08, "Designation of Senior Agency Officials for Privacy" (February 11, 2005) and section 522 of the Consolidated Appropriations Act of 2005 require Agencies to appoint a key Agency privacy official. However, although USAID designated a Senior Agency Official for Privacy (SAOP) and a Privacy Act Officer (PAO), neither was delegated authority over the Agency's privacy program, as required. The following section discusses this issue in detail.

Executive Order 13353, Section 1 (August 27, 2004) was enacted to:

> …protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions.

OMB Memorandum M-05-08, implemented Executive Order 13353, Section 1. The Memorandum required each Agency to appoint a senior official who will have overall agency-wide responsibility for information privacy issues. According to the Memorandum, that appointee should be the Agency's Chief Information Officer or another senior official at the Assistant Secretary equivalent level. Further, the Memorandum states that:

> …the senior agency official will have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

In addition, the Memorandum states that the Senior Agency Official for Privacy (SAOP) shall have a central role in overseeing, coordinating, and facilitating the agency's compliance efforts.

In July 2005, USAID appointed a SAOP, who assumed overall responsibility for policy relating to Agency information privacy issues, including collection, use, sharing, and disclosure of personal information. However, the Agency did not give the SAOP authority to oversee USAID's privacy program as required by OMB Memorandum M-05-08. For example, USAID's SAOP was not given responsibility for:

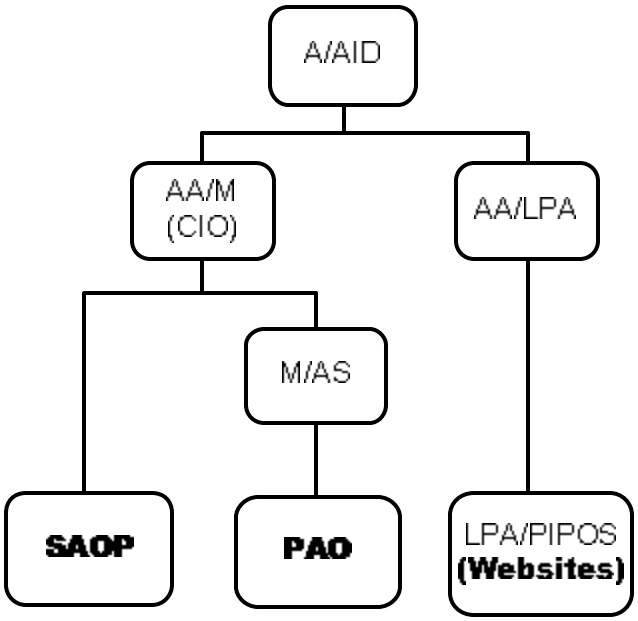
- Reviewing the Agency's information privacy procedures.
- Identifying methods to use technology to reinforce and sustain the privacy of personal information.

- Ensuring privacy training and education for Agency employees and contractors.
- Conducting periodic reviews to promptly identify privacy deficiencies, weaknesses, or risks.

In addition, although the SAOP was given responsibility for reviewing information privacy policy issues, the SAOP did not have overall authority to manage USAID's privacy program.

As a result of not being assigned all of the privacy roles and responsibilities identified in OMB Memorandum M-05-08, the SOAP could not enforce privacy requirements. For example, the SAOP developed privacy impact assessments (PIAs) for nine of USAID's critical systems which collect personally identifying information. The PIAs were provided to the appropriate privacy official so that they could be processed and published in the Federal Register. However, the SAOP later learned that, due to other priorities, the PIAs were not processed for publication in the Federal Register. Moreover, the SAOP did not have the authority to enforce the requirement to process and publish the PIAs because, as illustrated in Chart 1 below, he did not have a direct line of authority to require other privacy officials, such as the Privacy Act Officer (PAO) and the official in charge of websites, to meet privacy requirements.

Chart 1. USAID's Privacy Related Offices



Legend:
A/AID.....Office of the Administrator
AA/LPA.....Assistant Administrator, Bureau for Legislative and Public Affairs
AA/M.....Assistant Administrator, Bureau for Management
CIO.....Chief Information Officer
LPA/PIPOs.....Bureau for Legislative and Public Affairs, Public Information, Production and On-line Services Division
M/AS.....Bureau for Management, Administrative Services
PAO.....Privacy Act Officer
SAOP.....Senior Agency Official for Privacy

In addition, section 522 of the Consolidated Appropriations Act of 2005 requires that each agency have a Chief Privacy Officer (CPO) to assume primary responsibility for privacy and data protection policy. As of the date of this report, OMB has not issued implementing guidance for this Act.

In October 2005, USAID reported that the Agency had a CPO. However, it was later determined that rather than a CPO, USAID had a Privacy Act Officer who was appointed in August 1994. That Privacy Act Officer was responsible for:

- Authorizing Privacy Act requests for the Agency.
- Participating in the Agency's Privacy Working Group.
- Updating the Automated Directives System (ADS) Chapters (508 and 509).

However, the above responsibilities do not encompass all of the responsibilities of a CPO identified in section 522 of the Consolidated Appropriation Act of 2005. For example, the Privacy Act Officer did not have responsibility for:

- Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974.

- Conducting a privacy impact assessment of proposed rules of the Agency on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected.

- Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies.

- Ensuring that the Agency protects information in an identifiable form from unauthorized access, use, disclosure, disruption, modification, or destruction.

- Preparing a report to Congress on an annual basis on activities of the Agency that affect privacy, including complaints of privacy violations, internal controls, and other relevant matters.

As a result of not having a key Agency privacy official in place, USAID did not have an individual with the authority to implement and enforce an Agency-wide privacy program. Moreover, USAID did not have an individual that could be held accountable for ensuring that the Agency adequately protected privacy information about members of the public. Therefore, we are making the following recommendation.

> *Recommendation No. 1: We recommend that USAID's Assistant Administrator for the Bureau for Management, in collaboration with the Assistant Administrator for Legislative and Public Affairs, request that USAID's Administrator appoint a senior-level, key Agency privacy official with full authority to develop and implement USAID's privacy program.*

(Subsequent to the issuance of our draft report, we added the word "full" to Recommendation No. 1 to clarify the intent of the recommendation. USAID officials agreed with this change.)

Assignment of Other Privacy Roles and Responsibilities Needed - USAID's ADS 508, "Privacy Act 1974," assigns responsibility for the Agency to meet requirements of the Privacy Act of 1974. Specifically, ADS 508 assigns roles and responsibilities to officials, including:

- Director, Office of Administrator Services.
- General Counsel, Ethics/Administration.
- Privacy Officer.
- Privacy Act Implementation Officer.
- Privacy Coordination Officer.

However, according to the Privacy Act Officer, USAID's privacy roles were:

- Chief Information Officer.
- Privacy Act Officer.
- Chief Privacy Officer.
- Senior Official for Privacy.
- Privacy Advocate.

Further, in an October 2005 report[2] to OMB, USAID's key privacy roles were identified as:

- Agency Head.
- Chief Information Officer.
- Agency Inspector General.
- Chief Information Security Officer.
- Senior Agency Official for Privacy.
- Chief Privacy Officer.
- Reviewing Official for privacy impact assessments.

As shown in the preceding paragraphs, USAID's privacy roles need to be clearly defined and updated. Moreover, once the roles are defined, the corresponding responsibilities need to be determined. However, according to USAID officials, these updates were not made because adequate staff and resources were not available to carry out the privacy functions.

As a result of not clearly assigning roles and responsibilities, USAID can not fully implement an Agency-wide privacy program to protect personally identifying information about the public. Therefore, we are making the following recommendation.

> *Recommendation 2: We recommend USAID's key Agency privacy official clearly assign privacy roles and define the corresponding responsibilities.*

USAID Needs a Comprehensive Set of Privacy Policies and Procedures - According to GAO's "Standards for Internal Control in the Federal Government," management is responsible for developing detailed policies, procedures, and practices to fit their agency's operations and to ensure that they are built into an integral part of operations. Policies and procedures are control mechanisms that enforce management's directives to ensure that actions are taken to address risks.

[2] This information was reported in USAID's fiscal year 2005 Federal Information Security Management Act and Privacy Management Report.

However, as discussed below, USAID did not have a comprehensive set of privacy policies and procedures. Specifically, USAID's privacy policies and procedures were not fully referenced to other requirements. In addition, USAID did not have procedures for conducting privacy impact assessments and responding to privacy violations. [See "Cause of Problems Identified" section (pages 13-14) for a discussion of the reason USAID did not have a comprehensive set of privacy policies and procedures in place.]

Privacy Policies and Procedures Need to be Fully Referenced to Other Requirements – According to ADS 501, "The Automated Directives System," mandatory references to the ADS comprise of external references as well as Agency guidance that must be adhered to. In addition, according to "The ADS Process: A Mandatory Reference for ADS Chapter 501," such references must be cited in ADS chapters and will be hyperlinked.

USAID's privacy policies and procedures are described in various ADS chapters, interim updates, and Agency notices. However, the privacy policies and procedures were not fully referenced to indicate that other privacy policies exist.

For example:

- ADS 508, "Privacy Act – 1974," section 508.5.6, states that USAID shall publish in the Federal Register a description of each system of records that the Agency maintains. In addition, ADS 509, "Creating, Altering, or Terminating a System of Records (Records Pertaining to Individuals)," outlines the policies and essential procedures for the creation, alteration, or termination of a System of Records that meets the requirements of the Privacy Act. However, there were no references between the two chapters to indicate to the reader that USAID had additional policies and procedures for Systems of Records.

- ADS 557, "Public Information," was established to, among other things, provide the policy for Agency information distributed to the public, including via the Internet. In addition, Interim Update 04-01, "Updated Privacy Policy for USAID Information Technology Systems, Including Publicly Accessible Web Sites," was issued to alert USAID employees and contractors of their responsibilities under the E-Government Act of 2002 for, among other things, designing and creating web pages and web sites. However, although the Interim Update states that it is a mandatory reference to ADS 557, the Interim Update was not referenced in ADS 557.

As such, because the policies were not fully referenced, readers could easily overlook other critical aspects that were needed to meet privacy requirements. Although, on USAID's intranet, the ADS home page referenced some of its privacy policies, we are making the following recommendation to assist USAID in referencing its privacy policies and procedures.

> *Recommendation No. 3: We recommend that USAID's key Agency privacy official completely reference the Agency's privacy policies and procedures to other requirements in the Automated Directives System.*

Procedures for Privacy Impact Assessments Needed – OMB defined a privacy impact assessment (PIA) as an analysis of how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The E-Government Act of 2002, requires Agencies to complete PIAs prior to (1) developing or procuring information technology systems or projects that collect, maintain or disseminate information in identifiable form about an individual, or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons excluding agencies, instrumentalities or employees of the federal government. Specifically, Agencies are required to:

- Conduct PIAs.
- Ensure the Chief Information Officer (or equivalent official) reviews the PIAs.
- Make the PIAs publicly available through the website of the agency, publication in the Federal Register, or other means.

In addition, OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (September 26, 2003) requires that PIAs be performed and updated, as necessary, when a system change creates new privacy risks.

USAID has various policies that describe PIAs. Specifically:

- ADS 545.3.1.6, "System Development Life Cycle (SDLC) Planning," makes the system owner responsible for conducting PIAs.
- USAID's Interim Update 04-01, "Updated Privacy Policy for USAID Information Technology Systems, Including Publicly Accessible Web Sites" alerted USAID employees and contractors who develop or manage information technology on behalf of USAID of their responsibilities to perform PIAs as described in OMB M-03-22 (discussed above).
- Mandatory references to ADS 577, "Information Technology Capital Planning and Investment Control," require that, as part of the information technology investment process, a determination be made as to whether a PIA has been conducted.

(USAID also has a handbook that discusses some aspects of conducting PIAs, but the handbook was not up-to-date and was not incorporated into official Agency policy and procedures). However, none of the aforementioned policies describe procedures to ensure PIAs are conducted when required. Specifically, the policies do not address:

- How the complete inventory of systems of records will be obtained and maintained.
- What collection of personal information (e.g., name, address, phone number, e-mail address) maintained in a system necessitates the need for a PIA.
- Who within the Agency has overall responsibility for ensuring that PIAs are conducted and made available to the public.
- Who within the Agency is responsible for reviewing and approving PIAs.
- Who the PIAs must be submitted to upon completion.
- What mechanism the Agency will use to make the PIAs available to the public.

As a result of the above deficiencies, USAID did not have a complete inventory of systems requiring PIAs. Moreover, USAID could not assure that PIAs were conducted and made available to the public, when required. This problem was particularly prevalent with respect to

Agency websites—many of which collected personally identifying information from the public, such as names, addresses, phone numbers, and e-mail addresses. For example, one website collected personal information from users who were ordering products. Another website collected personal information from users who provided comments, suggestions or questions. Yet another site collected personal information when the user created a new account for giving monetary donations. Therefore, we are making the following recommendation.

> *Recommendation No. 4: We recommend USAID's key Agency privacy official develop and implement Agency-wide procedures for performing privacy impact assessments.*

Privacy Violation Response Procedures Needed – According to GAO's "Standards for Internal Control in the Federal Government," internal controls deficiencies should be communicated to the individual responsible for the function and also to at least one level of management above that individual. In addition, managers must take proper actions to ensure deficiencies are promptly resolved. Further, serious deficiencies should be reported to top management.

However, USAID did not develop procedures for responding to privacy violations. For example, USAID did not:

- Identify the offices (such as the Bureau for Legislative and Public Affairs, the Office of General Counsel, Office of Inspector General, Office of Information Resources Management, Office of Security, or Office of Human Resources) that should be contacted when a violation is identified.
- Determine the roles and responsibilities of the various offices involved in responding to privacy violations.
- Describe the type of information that should be reported.
- Determine how lessons learned will be communicated (e.g., via training) to prevent future reoccurrences of similar privacy violations.

For example, two websites were identified that inappropriately tracked users. In response, the Chief Information Officer's staff began to work with owners of the websites to correct the problems. However, when the incidents were brought to the attention of an Legislative and Pubic Affairs official, he thought that it was his office's responsibility to work with the owners of the website to correct the problem. Subsequently, upon reviewing Interim Notice #34, "USAID's Division of Responsibilities for USAID External Web Site," (July 12, 2000) that official agreed that it was not clear who was responsible for working with the website owners to correct the problems.

Without clear procedures for responding to privacy violations, USAID personnel were not informed of what actions should be taken to communicate and correct privacy problems. Moreover, USAID did not have a clear mechanism in place to prevent future recurrences of similar problems. Therefore, we are making the following recommendation.

Recommendation No. 5: We recommend that USAID's key Agency privacy official develop and implement procedures for responding to privacy violations. At a minimum, the procedures should include:

- *Identifying the offices that should be contacted when a violation is identified.*
- *Determining the roles and responsibilities of the various offices involved in responding to privacy violations.*
- *Describing the type of information that should be reported.*
- *Determining how lessons learned will be communicated to prevent future reoccurrences of similar privacy violations.*

(Subsequent to the issuance of our draft report, we added the second sentence to Recommendation No. 5 and the corresponding bullets to help ensure that USAID's planned corrective actions would be responsive to the problems discussed in the report. USAID officials agreed with this change.)

USAID Needs a Privacy Training and Awareness Program - GAO Standards for Internal Control in the Federal Government requires that management ensure that its workforce's skills are continually assessed. Training should be aimed at developing and retaining employee skill levels to meet challenging organizational needs.

However, USAID did not have a privacy training program in place. Specifically, although USAID developed 16 privacy Tips of the Day[3] for creating an awareness of privacy requirements to network users, only two were approved by the Office of the General Counsel for distribution to USAID employees. Moreover, those two tips were not distributed to all USAID personnel. As a result of not having a privacy training and awareness program, USAID's employees did not comply with requirements for protecting the privacy of the public. For example:

- PIAs were not always conducted on systems that collected personally identifying information.
- System of Records Notices were not always published in the Federal Register.
- Websites did not always contain required privacy policy disclosures.
- Unapproved tracking mechanisms were identified on USAID websites.

Therefore, the privacy of the public was not fully protected. [See "Cause of Problems Identified" section (pages 13-14) for a discussion of the reason USAID did not have a privacy training and awareness program in place.] As such, we are making the following recommendation.

Recommendation No. 6: We recommend that USAID's key Agency privacy official develop and implement an Agency-wide privacy training program.

USAID Needs a Process to Monitor Compliance With Privacy Requirements - GAO Standards for Internal Control in the Federal Government states that ongoing monitoring of internal controls should occur in the course of normal operations and should be built into the agency's operations. It also states that monitoring of internal control should include policies and procedures for ensuring that problems identified are promptly corrected.

[3] Tips of the Day provide daily computer security reminders to USAID network users.

However, as discussed below, USAID needs to develop and implement a process to ensure ongoing monitoring of its privacy program. [See "Cause of Problems Identified" section (pages 13-14) for a discussion of the reason USAID did not have a process in place to monitor compliance with privacy requirements.]

Monitoring Updates and Creation of System of Records Notices – According to the Privacy Act of 1974, each Agency that maintains a system of records must publish notification in the Federal Register upon establishment of the system. In addition, the notice must be revised when the system is modified.

In addition, ADS 509, "Creating, Altering, or Terminating a System of Records (Records Pertaining to Individuals)," outlines the policies and essential procedures for the creation, alteration, or termination of a System of Records that meets the requirements of the Privacy Act.

However, USAID did not follow its procedures to update its System of Records Notices (SORNs), when required. As such, the SORNs, dated March 31, 1980, were not updated to reflect the Agency's current systems of records. For example, the SORNs currently published in the Federal Register, state that several of the systems of records are located in offices that USAID no longer occupies in Virginia and Washington, D.C. However, the required updates to the records were not made and published in the Federal Register. In addition, USAID recently conducted PIAs for nine systems of records, but did not prepare and publish SORNs in the Federal Register.

As a result of not monitoring the updating and publishing of SORNs, the public was not made aware of the types of personally identifying information that USAID maintained. Therefore, we are making the following recommendation.

> *Recommendation No. 7: We recommend that USAID's key Agency privacy official develop and implement a process to monitor the timely preparation and publishing of System of Records Notices in the Federal Register.*

Monitoring of Websites – ADS 557, "Public Information," (July 25, 2000) provides USAID's policy for, among other things, Agency information distributed to the public. According to that policy, USAID's Bureau for Legislative and Public Affairs is responsible for reviewing Agency produced or funded materials available to the public on the Internet. The policy also states that USAID Bureaus, Offices, and officers are responsible for submitting Agency-funded or produced material for review prior to posting it to the Internet.

In July 2002, USAID issued an interim update No. 34 to ADS 557 "Division of Responsibilities for USAID External Web Site." That interim update was issued to restate the division of responsibility for the USAID external web site and to amplify the matters in ADS 557. However, the interim update discusses only USAID's external web site (i.e., www.usaid.gov), as opposed to all USAID-funded websites as discussed in ADS 557.

As such, USAID performed extensive monitoring to ensure that information posted on USAID's external web site met requirements. For example, USAID performed (1) content and technical reviews, including the privacy policy, before pages were added to the website and (2) periodic scans to determine whether unauthorized persistent mechanisms were placed on the site.

In contrast, USAID only recently began to perform limited monitoring for other Agency-funded websites. Specifically, after this audit began, USAID took initial steps to start scanning other Agency-funded websites for inappropriate tracking mechanisms. However, USAID did not monitor the content of those websites, such as the privacy policies. According to a Bureau for Legislative and Public Affairs official, USAID would need additional staff and funding to monitor all of the Agency-funded websites.

As a result, privacy problems were prevalent on other Agency-funded websites. For example, of the 13 websites selected for review:

- Three (23 percent) did not have the privacy policy posted on the website to inform the user of the nature, purpose, use and sharing of personally identifying information that is collected by the Agency. Moreover, seven of the websites (54 percent) with privacy policies posted did not make most of the disclosures required by OMB Memorandum M-03-22" OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (September 26, 2003). Such disclosures not made included notifying visitors of their privacy rights and what personally identifying information is collected. However, the privacy policy posted on USAID's external website made most of the required disclosures.

- Two (15 percent) placed unapproved tracking mechanisms on the user's computer. In addition, eight (62 percent) websites left the USAID-funded website—without a warning—and launched other websites that placed tracking mechanisms on the user's computer. However, no problems were identified with USAID's external website.

- Twelve (92 percent) of the websites were not on the .gov domain as required by USAID's November 28, 2005, Policy Notice, "USAID Websites and .gov Domains." According to OMB M-05-04 "Policies for Federal Agency Public Websites, " December 17, 2004, hosting the websites on the .gov domain provides the public clear, unambiguous notification of the Agency's sponsorship of the website. By not hosting the websites on the .gov domain, members of the public were not assured that the websites—most of which collected personally identifying information—were official Agency websites.

As such, the privacy of public users was sometimes invaded when using other Agency-funded websites. Moreover, such site users were not always made aware of how such personally identifying information would be used, if collected.

Although USAID has begun to take some actions to monitor other Agency-funded websites, we are making the following recommendation to help the Agency ensure the protection of the public's privacy when using Agency-funded websites.

> *Recommendation No. 8: We recommend that USAID's key Agency privacy official establish a process to monitor Agency-funded websites to ensure the privacy of website users is protected.*

Cause of Problems Identified – USAID management was aware of the weaknesses in its privacy program. However, as discussed below, corrective action was not taken because privacy was not considered a priority for the Agency.

In the past few years, several reports and reviews have been conducted that identified weakness in USAID's privacy program. For example, in December 2001, a USAID contractor reported on its evaluation of gaps in USAID's systems of records and privacy program. That report determined that, USAID's:

- Infrastructure for complying with privacy requirements was immature.
- Implementation and operations of the privacy policies was inconsistent.
- Approach to privacy needed to be customer-oriented, such as by providing training and awareness.

As such, the report made several recommendations for USAID to improve on areas of the privacy program, including the responsibility and organization, training, accountability, policy, and compliance. Additionally, the report made numerous recommendations to address specific non-compliance issues, such as with deficiencies in system of record notices.

In addition, on September 11, 2002, the Office of Inspector General issued "Risk Assessment of Major Functions Within the Information and Records Division of the Office of Administrative Services, Bureau for Management" (Report No. A-000-02-003-S). That report concluded that some ADS chapters were outdated and the Agency's system of record notices needed to be updated. Therefore, the report suggested that the Office of Administrative Services institute improvements regarding the ADS chapters and the inventory of systems of records. USAID management agreed with the suggested course of actions for the ADS chapter. However, for the systems of records notices, USAID management responded that there were not enough manpower resources to correct this inadequacy.

In addition, although USAID management was aware of the weaknesses in its privacy program, correcting the weaknesses was not a USAID priority. For example, USAID's prior Senior Agency Official for Privacy developed a privacy upgrade Action Plan, dated March 1, 2001. That action plan identified some of the same problems identified in this audit, such as the need to (1) clarify privacy roles and responsibilities, (2) implement a privacy training and outreach program, and (3) document an integrated privacy policy for the Agency. However, according to USAID management, staffing and funding limitations precluded the Agency's ability to implement a privacy program.

Nonetheless, in recent years, Congress, OMB, and private interest groups have directed an increased focus on privacy issues. For example, Section 522 of the 2005 Consolidated Appropriations Act requires the Inspector General to conduct an annual review of agency privacy practices.

Therefore, we believe it is imperative that USAID managers continue to better prioritize the workload and mandatory tasks. Specifically, USAID needs to implement an Agency-wide privacy program to meet the mandated requirements to protect the privacy of the public and, thus, protect the Agency's reputation. Due to the extensive weaknesses identified in USAID's privacy program, Agency officials need to make privacy a priority by promptly taking corrective actions to address the recommendations made in this audit report. Thus, USAID should recognize its privacy program as a reportable condition to be internally tracked and monitored until the weaknesses are corrected.

Recommendation No. 9: We recommend that USAID's key Agency privacy official request that the Management Control Review Committee review the Agency's privacy program and consider reporting, tracking, and monitoring its weaknesses as a reportable condition for the Agency.

EVALUATION OF MANAGEMENT COMMENTS

USAID management agreed to take corrective action on all nine recommendations in the report. For Recommendation Nos. 2, 3, 4, 5, 6, 7, 8, and 9, USAID management provided corrective action plans and target completion dates. Therefore, we consider that management decisions have been reached for the above recommendations. In addition, based on the response and supporting documentation provided, final action has been taken on Recommendation No. 1 upon issuance of this report. Specifically, we recommended that Agency officials request USAID's Administrator to appoint a senior-level, key Agency privacy official with full authority to develop and implement USAID's privacy program. In response, Agency officials requested that USAID's Administrator appoint a Chief Privacy Officer to assume primary responsibility for establishing the Agency's privacy program in accordance with privacy laws and regulations.

Aside from addressing the recommendations, USAID management stated that the discussion about the use of non-.gov domains for Agency funded websites (before recommendation no. 8), is not relevant to the privacy of information technology systems. However, we believe that maintaining websites on the .gov domain as required provides a level of assurance to users that the site is an official USAID website—especially if the user chooses to provide personally identifying information. Although we did not remove this discussion from the audit report, we referenced OMB M-05-04, "Policies for Federal Agency Public Websites, " December 17, 2004, which states that hosting the websites on the .gov domain provides the public clear, unambiguous notification of the Agency's sponsorship of the website.

The complete text of USAID's management comments is included in Appendix II.

SCOPE AND METHODOLOGY

Scope

The Office of Inspector General, Information Technology and Special Audits Division conducted this audit in accordance with generally accepted government auditing standards. The purpose of the audit was to determine whether USAID implemented key components of a privacy program. Audit fieldwork was conducted at USAID headquarters in Washington, D.C., from December 6, 2005 through April 5, 2006.

The audit included a follow up on prior audit recommendations contained in Report No. A-00-01-001-P, "Audit of USAID's Compliance with Internet Privacy Policies," dated May 14, 2001).

In addition, we tested the following internal controls in USAID's privacy program:

- Privacy management structure.
- Policies and procedures, including violation response.
- Awareness and training.
- Monitoring compliance.

Methodology

To determine if USAID implemented key components of a privacy program we obtained and reviewed the following laws and regulations: E-Government Act of 2002; The Privacy Act of 1974; and the Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," dated September 26, 2003.

In addition, we conducted interviews with key USAID privacy personnel in the Bureau for Management, Office of Administrative Services; Office of the Chief Information Officer; Bureau of Legislative and Public Affairs; and Office of General Counsel. However, we did not interview or evaluate Privacy Liaison Officers at USAID Missions.

We asserted the necessary components of a privacy program are (1) privacy management structure (including clear assignment of roles and responsibilities), (2) policies and procedures (including violation response), (3) awareness and training, and (4) monitoring compliance. For each component, we obtained and reviewed USAID documents including, but not limited to: (1) privacy impact assessments, (2) Privacy Tips of the Day, (3) System of Records Inventory, (4) System of Records Notices, and (5) USAID's privacy policies and procedures.

Finally, although USAID's universe of websites was incomplete, we selected a judgmental sample of 13 USAID funded-websites that contained USAID's logo and were updated as of September 1, 2005, and tested compliance with privacy policy disclosures and use of tracking mechanisms.

MANAGEMENT COMMENTS

May 23, 2006

MEMORANDUM

TO: IG/A/ITSA, Melinda A. Dempsey

FROM: C/AID, Mosina Jordan "/s/"
AA/LPA, J. Edward Fox "/s/"

SUBJECT: Management Response to the OIG Draft Report on the Audit of USAID's *Implementation of Key Components of a Privacy Program for its Information Technology Systems* (Report No. A-000-06-00X-P)

Thank you for the opportunity to respond to the draft audit report. This memorandum contains the management decisions for the Draft Audit of USAID's *Implementation of Key Components of a Privacy Program for its Information Technology Systems*.

There is one issue outside the recommendations that we would like to bring to your attention for consideration. This issue is described at the end of management's responses to the recommendations. Management would appreciate if the audit team could consider this issue and make appropriate changes while finalizing its audit report.

The following are our management decisions and corrective actions regarding the proposed audit recommendations:

Recommendation No. 1: We recommend that USAID's Assistant Administrator for the Bureau for Management, in collaboration with the Assistant Administrator for Legislative and Public Affairs, request that USAID's Administrator appoint a senior-level, key Agency privacy official with full authority to develop and implement USAID's privacy program.

Management Response: An Action Memorandum to the Administrator, was sent from Mosina Jordan and Edward Fox, the Bureaus for Management and Legislative and Public Affairs requesting the Administrator's appointment of a Chief Privacy Officer (CPO).

We request closure of Recommendation One upon issuance of the final audit report. A copy of the executed Memoranda is attached.

Recommendation 2: We recommend USAID's key Agency privacy official clearly assign privacy roles and define the corresponding responsibilities.

Management Response: The USAID CPO will issue a new ADS Chapter, **USAID Privacy Program**, to assign the Agency's privacy roles and define corresponding responsibilities. (October 2006)

Recommendation No. 3: We recommend that USAID's key Agency privacy official completely reference the Agency's privacy policies and procedures to other requirements in the Automated Directives System.

Management Response: The new ADS Chapter, **USAID Privacy Program**, will reference USAID privacy-related policies and procedures in the Automated Directives System (ADS), as well as OMB privacy policy directives. (October 2006)

Recommendation No. 4: We recommend USAID's key Agency privacy official develop and implement Agency-wide procedures for performing privacy impact assessments.

Management Response: The USAID CPO will develop formal procedures for performing privacy impact assessments as supporting documentation to the new ADS Chapter on Privacy. The existing draft Privacy Impact Assessment (PIA) template used for PIAs will be incorporated as part of this procedure document. (October 2006)

Recommendation No. 5: We recommend that USAID's key Agency privacy official develop and implement procedures for responding to privacy violations. At a minimum, the procedures will include:

- Identifying offices that must be contacted when a violation is identified;
- Determining the roles and responsibilities of the offices involved in responding to privacy violations;
- Describing the type of information that should be reported; and
- Determining how lessons learned will be communicated to prevent future reoccurrences of similar privacy violations.

Management Response: The USAID CPO will develop a supporting document to the new ADS Chapter on Privacy that defines procedures for responding to privacy violations. (October 2006). At a minimum, the procedures will include:

- Identifying offices that must be contacted when a violation is identified;
- Determining the roles and responsibilities of the offices involved in responding to privacy violations;
- Describing the type of information that should be reported; and
- Determining how lessons learned will be communicated to prevent future reoccurrences of similar privacy violations.

Recommendation No. 6: We recommend that USAID's key Agency privacy official develop and implement an Agency-wide privacy training program.

Management Response: The USAID CPO will develop an Agency-wide privacy training program. Current implementation of the security awareness training includes elements of the

privacy program. This will be more fully expanded. (October 2006)

Recommendation No. 7: We recommend that USAID's key Agency privacy official develop and implement a process to monitor the timely preparation and publishing of System of Records Notices in the Federal Register.

Management Response: The USAID CPO will develop a process to monitor the timely preparation and publishing of System of Records Notices in the Federal Register. The process will be defined in the new ADS Chapter on Privacy. (October 2006)

Recommendation No. 8: We recommend that USAID's key Agency privacy official establish a process to monitor Agency-funded websites to ensure the privacy of website users is protected.

Management Response: The USAID CPO, in coordination with the review process outlined in ADS 557, will establish a process to monitor Agency-funded websites, ensuring privacy protection of website users. (October 2006)

Recommendation No. 9: We recommend that USAID's key Agency privacy official request that the Management Control Review Committee (MCRC) review the Agency's privacy program and consider reporting, tracking, and monitoring its weaknesses as a reportable condition for the Agency.

Management Response: The USAID CPO will report progress on the recommendations in this report to the MCRC for review before their next meeting. The CPO's report will permit MCRC to track, monitor and determine whether progress of USAID's privacy program in resolving weaknesses is a reportable condition. (September 2006)

Issue for Consideration Outside Recommendations: Management notes that in the discussion before recommendation 8, the audit team discusses USAID-financed websites on non-.gov domains. We do not view this discussion—in the context of privacy issues—as relevant to the topic of privacy of information technology systems. The Office of Management and Budget, in OMB Memorandum 05-04, frames the .gov issue in the terms of information quality and information assurance—not in terms of privacy. Residing on a .gov domain has no impact on one way or the other on the privacy of an information technology system user. Management requests that this discussion be removed from the draft report as not relevant to the immediate decision.

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