Office of Inspector General

December 19, 2006

MEMORANDUM

TO: M/AA Chief Privacy Officer, Phil Heneghan

FROM: IG/A/ITSA Director, Melinda G. Dempsey /s/

SUBJECT: Independent Auditor's Report on Applying Agreed-Upon Procedures for Assessing USAID's Implementation of Section 522 of the Consolidated Appropriations Act of 2005 (Report No. A-000-07-002-O)

This memorandum transmits our final report on the subject assessment for your review and comment. (See Appendix for a discussion about this Agreed-Upon Procedures Report.) Although this is not an audit report, we are making six recommendations, which will be tracked in the Consolidated Audit Tracking System. Based on the supporting documentation already provided, we consider that final action has been taken on Recommendation No. 3 as of the date of this memorandum.

The United States Agency for International Development's (USAID) Office of Inspector General, Information Technology and Special Audits Division, engaged Urbach Kahn & Werlin, LLP, to conduct an independent assessment to determine USAID's compliance with §522 of the Consolidated Appropriations Act of 2005. The fieldwork was conducted at USAID's Headquarters in Washington D.C. between September 29, 2006, and November 20, 2006. The specific objective of the assessment was to answer the following question:

Did USAID develop and implement comprehensive privacy and data protection procedures as required by the Consolidated Appropriations Act of 2005, §522?

Enacted on December 8, 2004, Consolidated Appropriations Act of 2005 (Public Law 108-447), Division H, Title V, §522 (hereafter referred to as §522), requires that each Agency designate a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy. The Act also requires each agency to:

- Establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public.

- Prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the

Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report.

- Have an independent third-party review performed at least every two years on the agency's use of information in an identifiable form.

Urbach Kahn & Werlin, LLP, determined that, although USAID has made positive strides over the past year to address privacy related weaknesses, all of the key requirements of the Consolidated Appropriations Act of 2005, §522, were not met. Specifically, USAID did not:

- Finalize the Agency's comprehensive privacy policies and procedures.

- Complete its inventory of systems that contain personally identifiable information and update its system of record notices to reflect the Agency's current systems of records.

- Consistently perform and fully document its Privacy Impact Assessments.

- Complete its inventory of Agency-funded websites.

- Prepare a report of its use of information in an identifiable form along with its privacy and data protection policies and procedures.

- Implement role-based training for individuals responsible for Personally Identifiable Information.

These weaknesses occurred because the privacy program was not considered a priority in years past. As a result of these weaknesses, USAID has not mitigated the risk of privacy-related vulnerabilities and inadvertent release of information in an identifiable form. Therefore, we are making the following recommendations, which will be included in the Consolidated Audit Tracking System, and which will therefore require management decisions by USAID.

Recommendation No. 1: We recommend that USAID's Chief Privacy Officer complete and finalize the revised privacy policies and procedures that encompass a more comprehensive approach to privacy compliance.

Recommendation No. 2: We recommend that the USAID's Chief Privacy Officer provide training and guidance on accurately completing privacy impact assessments to personnel responsible for conducting and preparing privacy impact assessments.

Recommendation No. 3: We recommend that the system owner for the Office of Foreign Disaster Assistance network in conjunction with the Chief Privacy Officer, complete privacy impact assessments for the databases maintained on the Office of Foreign Disaster Assistance network.

Subsequent to the issuance of the draft report, USAID completed a privacy impact assessment for the database on the Office of Foreign Disaster network. Based on the supporting documentation provided to Urbach Kahn & Werlin, LLP, final action has been reached on Recommendation No. 3 upon issuance of this report.

> Recommendation No. 4: We recommend that USAID's Chief Privacy Officer, in collaboration with the Bureau for Legislative and Public Affairs/Public Information, Production and Online Services, assemble a complete inventory of USAID-funded websites.
>
> Recommendation No. 5: We recommend USAID's Chief Privacy Officer complete the report of USAID's use of information in an identifiable form and record it with the Agency's Inspector General.
>
> Recommendation No. 6: We recommend that USAID's Chief Privacy Officer identify specific user roles requiring role-based training and develop and implement an agency-wide training program regarding role-based training for individuals responsible for personally identifiable information.

Urbach Kahn & Werlin, LLP's report in its entirety is attached to this report.

We request that you provide your comments to us within 30 days of the date of this memorandum. In your comments, we request that you clearly state your position on Recommendations Nos. 1, 2, 4, 5, and 6. If you agree with the recommendations, please confirm your agreement and include a plan for corrective action with a target date of completion for the planned action. If you disagree, please provide a detailed explanation of your reason.

I appreciate the cooperation and courtesy extended to my staff and our independent third-party contractor throughout the assessment.

ABOUT THIS AGREED UPON PROCEDURES REPORT

We have performed the procedures enumerated in the Consolidated Appropriations Act of 2005, §522, which were agreed to by the United States Congress. The purpose of the procedures was to:

- Measure actual privacy and data protection practices against the Agency's recorded privacy and data protection procedures.

- Ensure compliance and consistency with both online and offline stated privacy and data protection policies.

- Provide the Agency with ongoing awareness and recommendations regarding privacy and data protection procedures.

- Ensure the Agency's description of the use of [privacy] information in an identifiable form is accurate and accounts for the agency's current technology and its processing of information in an identifiable form.

USAID management is responsible for developing and implementing comprehensive privacy and data protection procedures.

This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and Government Auditing Standards, issued by the Comptroller General of the United States. The sufficiency of the procedures is the sole responsibility of the parties specified in this report. Consequently, we make no representations regarding the sufficiency of the procedures in the attachment for the purpose for which this report has been requested or for any other purpose.

We were not engaged to and did not conduct an audit, the objective of which would be the expression of an opinion on the adequacy of the controls. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended for the information and use of the United States Congress and the public.

Independent Assessment of the United States Agency for International Development's Compliance with §522 of the Consolidated Appropriations Act of 2005

Final Report

December 11, 2006

UK &W Urbach Kahn & Werlin LLP
CERTIFIED PUBLIC ACCOUNTANTS

Independent Assessment of the U.S. Agency for International Development's Compliance with §522 of the Consolidated Appropriations Act of 2005

TABLE OF CONTENTS

Executive Summary

The United States Agency for International Development's (USAID or the Agency) Office of Inspector General (OIG), Information Technology and Special Audits Division engaged Urbach Kahn & Werlin LLP (UKW) to conduct an independent assessment to determine USAID's compliance with §522 of the Consolidated Appropriations Act of 2005. The Consolidated Appropriations Act of 2005 requires that each agency designate a Chief Privacy Officer and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. (See page 2).

The assessment concluded that USAID did not meet all of the key requirements of *§*522 of the Consolidated Appropriations Act of 2005. The Agency has made positive strides over the past year to address privacy related weaknesses. However, USAID still faces several important challenges to refine its privacy program in order to mitigate the risk of privacy related vulnerabilities and inadvertent release of information in an identifiable form. For example:

- Comprehensive privacy policies and procedures were still in draft format and had not yet been finalized. (See page 5).

- USAID did not have a complete inventory of systems that contain personally identifiable information and system of record notices had not been updated to reflect the Agency's current systems of records. (See page 7).

- Privacy Impact Assessments had not been consistently performed and are not fully documented. (See page 8).

- USAID did not have a complete inventory of Agency funded websites. (See page 9).

- USAID had not prepared a report of its use of information in an identifiable form along with its privacy and data protection policies and procedures. (See page 12).

- USAID had not implemented role-based training for individuals responsible for personally identifiable information. (See page 12).

These weaknesses occurred because the privacy program was not considered a priority in years past. However, USAID has recently begun to take corrective action by appointing a Chief Privacy Officer with overall authority to develop and implement the Agency's privacy program in accordance with privacy laws and regulations.

This report contains six recommendations to help USAID improve its privacy program and practices.

Background

The United States Agency for International Development (USAID) is an independent Federal Agency responsible for conducting foreign assistance and humanitarian aid, advancing the political and economic interests of the United States. USAID, based in Washington, DC, operates in about 100 developing countries and provides assistance to these countries by supporting:

- Economic growth, agriculture, and trade;
- Global health; and
- Democracy, conflict prevention, and humanitarian assistance.

The Consolidated Appropriations Act of 2005 (Public Law 108-447), Division H Transportation/Treasury, Title V, §522 (hereafter referred to as §522), requires that each Agency designate a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy. The act also requires each agency to:

1. Establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public;
2. Prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report; and
3. Have an independent third party review performed at least every two years on the agency's use of information in an identifiable form.

Objective

Urbach Kahn & Werlin (UKW) was engaged by USAID's Office of Inspector General (OIG), Information Technology and Special Audits Division, to conduct an independent assessment to determine USAID's compliance with §522 of the Consolidated Appropriations Act of 2005. As a result, the objective of this review was to answer the following question:

> *Did USAID develop and implement comprehensive privacy and data protection procedures as required by the Consolidated Appropriations Act of 2005, §522?*

Scope

In assessing USAID's compliance with the requirements of §522, we evaluated the following areas:

- Reviewed documentation and reports from USAID/OIG privacy audits and assessments;
- Assessed USAID's privacy policies and procedures against existing privacy laws and regulations to identify gaps and inconsistencies;
- Analyzed two of USAID's networks, AIDNET and Office of Foreign Disaster Assistance (OFDANET), and a sample of eight USAID funded websites for privacy vulnerabilities in accordance with §522. These privacy vulnerabilities include noncompliance with stated practices, policies and procedures, as well as risks of inadvertent release of information in an identifiable form.

The fieldwork was conducted at USAID's Headquarters in Washington, D.C. between September 29, 2006 and November 20, 2006.

Testing Methodology

To determine if USAID implemented the requirements of the Consolidated Appropriations Act, §522, we reviewed privacy laws and regulations including, but not limited to: The Consolidated Appropriations Act of 2005; Privacy Act of 1974; Office of Management and Budget (OMB) Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;" and OMB Memorandum M-06-16, "Protection of Sensitive Agency Information."

We conducted interviews with key USAID privacy personnel including the Chief Privacy Officer/Chief Information Officer, Privacy Implementation Officer as well as representatives of the Bureau of Legislative and Public Affairs (LPA) and Office of the Chief Information Officer.

We obtained and reviewed USAID documents including, but not limited to:

- USAID's policies related to the agency's privacy program which include the *Automated Directive System (ADS) 545 - Information Systems Security* including the conforming amendments made to the policy*, ADS 557- Public Information*, *ADS Chapter 508 - PRIVACY ACT – 1974, and ADS Chapter 509 - Creating, Altering, or Terminating a System of Records (Records Pertaining to Individuals)*
- Privacy Impact Assessments
- Privacy Tips of the Day
- System of Records Inventory
- System of Records Notices (SORN)
- AIDNET and OFDANET System Security Documentation

We also analyzed eight USAID funded websites to identify privacy vulnerabilities. The websites were judgmentally selected in collaboration with the OIG. For the sample of websites, we tested the following: whether the websites were using Secure Socket Layer (SSL) to capture and transfer Privacy Act protected user data, whether the

appropriate privacy policy and disclosures were posted and available for all visitors and users of the websites, tested compliance with the use of tracking mechanisms, and ensured that any personal identifiable information was protected. The websites we selected for review included the following:

- http://www.eehicd.net
- http://www.usaidkenya.org
- http://www.usaidjordan.org
- http://ane-environment.net
- http://www.usaideasttimor.net
- http://www.usaid.gov
- http://africastories.usaid.gov
- http://www.usaidafghanistan.org

Findings and Recommendations

USAID did not meet all of the key requirements of the Consolidated Appropriations Act of 2005, *§*522. These weaknesses occurred because the privacy program was not considered a priority in years past. However, the Agency has made positive strides over the past year to address privacy related weaknesses. For example, USAID has recently appointed a Chief Privacy Officer with overall authority to develop and implement the Agency's privacy program in accordance with privacy laws and regulations. In addition, USAID has revised the main privacy policy document, ADS 508 – USAID Privacy Program, which provides a comprehensive set of privacy policies and procedures. However, the new ADS 508 is currently in draft form.

USAID still faces several important challenges to refine its privacy program in order to mitigate the risk of privacy related vulnerabilities and inadvertent release of information in an identifiable form. For example:

- Comprehensive privacy policies and procedures were still in draft format and had not yet been finalized.
- USAID did not have a complete inventory of systems that contain personally identifiable information and system of record notices had not been updated to reflect the Agency's current systems of records.
- Privacy Impact Assessments had not been consistently performed and are not fully documented.
- USAID did not have a complete inventory of Agency funded websites.
- USAID had not prepared a report of its use of information in an identifiable form along with its privacy and data protection policies and procedures.
- USAID had not implemented role-based training for individuals responsible for Personally Identifiable Information (PII).

These findings are further discussed below.

1. Comprehensive privacy policies and procedures were still in draft format and had not yet been finalized.

According to §522 of the Consolidated Appropriations Act of 2005, within 12 months of enactment of the Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.

During our review period, USAID had the following formally established and approved policies relating to the Agency's privacy program and practices:

- ADS 508 – Privacy Act of 1974
- ADS 509 – Creating, Altering or Terminating a System of Records
- ADS 557 – Public Information
- ADS 545 – Information Security (including Conforming Amendments)

During the course of the review, however, USAID provided a draft revision of the ADS 508. The draft version provided encompasses a more comprehensive approach to privacy compliance in comparison to the ADS 508 currently in place. The draft version that we reviewed replaces the old chapters and provides a clear definition of personal identifiable information, formal procedures for conducting privacy impact assessments, and incident response mechanisms in the event of privacy violations. Further, the new ADS 508 will reference other USAID privacy related policies and procedures as well as OMB privacy policy directives.

Due to the timing and scope of the current assessment, we reviewed the finalized policies listed above that are currently in place. While these policies are available via the Automated Directives System, they are not fully referenced to each other. Further, the current version of USAID's policies did not provide a clear definition of personally identifiable information (PII), outline formal procedures for conducting privacy impact assessments, or procedures for responding to privacy violations.

USAID management is aware of the weaknesses in its privacy program. According to a previous audit conducted by the USAID Office of Inspector General (OIG)[1], the privacy program was not considered a priority for the Agency in years past.

Without finalizing the draft privacy policies and procedures, users will not be aware of USAID's policies and procedures relating to the privacy and protection of personally identifiable information.

On June 8, 2006, the Office of Inspector General issued "Audit of USAID's Implementation of Key Components of a Privacy Program for its Information Technology Systems" (Report No. A-000-06-003-P). The report identified that USAID had not referenced the Agency's privacy policies and procedures to other requirements in the Automated Directives System, implemented formal procedures to conduct privacy impact assessments, or implemented formal procedures for responding to privacy violations. Since these issues had been addressed during the OIG Privacy audit, we are not making a recommendation in these areas.

However, we are making the following recommendation:

Recommendation No. 1

We recommend that USAID's Chief Privacy Officer complete and finalize the revised privacy policies and procedures that encompass a more comprehensive approach to privacy compliance.

[1] 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)

2. USAID did not have a complete inventory of systems that contain personally identifiable information and system of record notices had not been updated to reflect the Agency's current system of records.

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 and revise the notice if and when a change is made. USAID could not provide a complete inventory of USAID information systems that contain Personally Identifiable Information (PII). According to the Chief Privacy Officer, the inventory is still being constructed.

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. As reported in an OIG audit report[2], and as corroborated by the fieldwork conducted in this review, USAID did not follow its procedures (ADS 509 "Creating, Altering, or Terminating a System of Records) to update its System of Records Notices (SORNs), when required. As such, the SORNs have not been 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. During our review, we concluded that corrective action had not been completed on the reported finding.

According to USAID officials, the Chief Privacy Office is currently working on several new Systems of Records Notices including: 1) the Partner Vetting System, 2) the update to the Office of Security "umbrella" System of Records Notices, 3) the CISO Security Tips of the Day, and 4) the OFDA People Trak database. In addition, the Chief Privacy Office has received concurrence from the General Counsel that the Chief Privacy Office should reissue the existing SORNs for significantly altered System of Records.

USAID management is aware of the weaknesses in its privacy program. According to a previous audit conducted by the USAID OIG, the privacy program was not considered a priority for the Agency in years past.

As a result of not having a complete inventory of systems that contain PII and the lack of monitoring, updating and publishing of SORNs, the Agency and the public is not aware of the types of personally identifying information that USAID maintains.

On June 8, 2006, the Office of Inspector General issued an audit report[3] that identified that USAID had not monitored the timely preparation and publishing of System of Records Notices in the Federal Register. Additionally, the following OIG report "Agreed Upon Procedures for Assessing USAID's Protection of Remote use of

[2] 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)
[3] 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)

Personally Identifiable Information and Information Systems" (Memorandum Report No. A-000-07-001-S, November 28, 2006) identified that USAID did not have a complete inventory of systems that contain personally identifiable information. Therefore, we are not making a recommendation in these areas since the issues were addressed in previous OIG audits.

3. Privacy impact assessments had not been consistently performed and are not fully documented.

The E-Government Act of 2002 requires Agencies to complete Privacy Impact Assessments (PIA) 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.

Our review of the AIDNET and OFDANET Privacy Impact Assessments identified that the PIAs have not been properly completed. USAID provided us with the PIA templates for AIDNET and OFDANET; however, the information documented in the PIA templates for AIDNET and OFDANET differ from the summary PIAs that are posted on the USAID website. For example, the PIA templates for AIDNET and OFDANET state that PII is either contained or collected. However, the PIAs posted to the USAID privacy program webpage state that they do not. According to USAID officials, the information posted to the USAID privacy program webpage is correct because AIDNET and OFDANET do not contain or collect PII. In addition, the PIAs that have been completed do not contain the date they were signed off on, the signatures of appropriate personnel who are authorized to sign off on the completed PIA, and there is incomplete information in the comments sections where comments and guidance are used for further clarification for PIA steps.

Additionally, PIAs have not been completed for any of the databases maintained on OFDANET. These databases are: People Trak, Field Support (FST), and Disaster Assistance Support (DASP). We were informed by OFDANET officials that FST and DASP were recently discovered to be housed on OFDANET and they would complete PIAs for these databases.

USAID management is aware of the weaknesses in its privacy program. According to a previous audit conducted by the USAID OIG, the privacy program was not considered a priority for the Agency in years past. The Agency has recently begun implementing the privacy program. In addition, personnel responsible for completing PIAs had not received proper training and guidance to ensure PIAs were completed accurately.

Without a complete and accurate PIA, USAID will not be able to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an information system.

Recommendations No. 2

We recommend that the USAID's Chief Privacy Officer provide training and guidance on accurately completing privacy impact assessments to personnel responsible for conducting and preparing privacy impact assessments.

Recommendation No.3

We also recommend that the system owner for the Office of Foreign Disaster Assistance network in conjunction with the Chief Privacy Officer, complete privacy impact assessments for the databases maintained on the Office of Foreign Disaster Assistance network.

(Note: Subsequent to the issuance of the draft report, OFDANET officials reported that they had met with Office of the Chief Information Security Officer (CISO) personnel regarding the completion of privacy impact assessments for the OFDANET databases. Upon review of the OFDANET databases, it was determined that a privacy impact assessment would only need to be completed for the People Trak database. Therefore, a privacy impact assessment, System of Record and Notice (SORN), and System Classification was completed for the People Trak database. Based on the supporting documentation that was provided, this recommendation will be closed upon issuance of the final report.)

4. USAID did not have a complete inventory of Agency funded websites.

The ADS 557 – Public Information provides the policy directives for Agency information distributed to the public and details how to respond to requests from the public for information about USAID's programs and activities. According to ADS 557, USAID's Bureau for Legislative and Public Affairs is responsible for maintaining the Agency's inventory of public websites. However, USAID does not have a complete inventory of USAID funded websites. During the course of our review, we were provided two separate partial website inventories. One inventory is maintained by the USAID's Bureau of Legislative and Public Affairs and the second is maintained by the Office of the Chief Information Security Officer (CISO). However, these inventories have not been consolidated into one inventory.

USAID has recently begun to compile a complete inventory of USAID funded websites as well as a process to monitor the websites for privacy compliance. According to a representative from the Bureau of Legislative and Public Affairs, USAID would need additional staff and funding to monitor all Agency funded websites.

As a result, external USAID websites are partially in compliance with §522 of the Consolidated Appropriations Act of 2005, and OMB Memorandum 00-13 "Privacy Policies and Data Collection on Federal Web Sites." In the course of our review, we noted the following conditions on the websites selected for review:

- **Persistent Cookie** – The site, http://africastories.usaid.gov, set a persistent cookie while reviewing the site. This cookie was set to expire in 2036, which is a length of time customary for such cookies. During our review of the site, it was determined that the cookie requested no user specific information, but was being used to associate specific page views. No private information was seen to pass between web browser and the originating site. According to USAID officials, there is no waiver in place to use a tracking mechanism on this web site.

- **Web Bug**[4] – The site associated with http://ane-environment.net appears to set a cookie/bug which is associated to the Google search function on the page.

  According to M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below; agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:

  - the nature of the information collected;
  - the purpose and use for the information;
  - whether and to whom the information will be disclosed; and
  - the privacy safeguards applied to the information collected.

- **SSL Keys –** The sites, http://www.usaidafghanistan.org and http://www.usaidkenya.org, offer Secure Socket Layer functionality to site users. In both cases, the keys present were un-trusted, being self-signed and related to other web sites. This state negates the security and trust relationship provided to the end-user. Because the key is not associated with the site of origin, the end-user cannot establish the authenticity of the key. According to National Institute of Standards and Technology (NIST) Special Publications 800-44, *Guidelines on Securing Public Web Servers*, "without some process to authenticate the server, users of the public Web server will not be able to determine if the server is the "authentic" Web server or a counterfeit version operated by a malicious entity."

- **User Information –** It was possible to find information regarding program participants by following a link off the http://ane-environment.net site. This information included program participants and personal contact information.

[4] A Web bug is a graphic on a Web page designed to monitor who is reading the page or message. Web bugs are often invisible because they are typically only 1-by-1 pixels in size. In many cases, Web bugs are placed on Web pages by third parties interested in collecting data about visitors to those pages.

- **Administrative Information** – It was possible to view potential private and system administrative information by following a link off the http://www.eehicd.net site to a training contractor, http://egypt.usaidtraining.devis.com.

- **Site Warning Banner** – Four of eight websites tested; http://www.eehicd.net, http://www.usaidkenya.org, http://www.usaidjordan.org, and http://www.usaideasttimor.net do not warn visitors that they are leaving the site when activating an on-site link. According to Technical Regulations for AID/Washington external website pages per the Xweb guidance, all links to sites not residing on a .gov server must utilize the "Goodbye" script.

- **Privacy Notice –** The site, http://www.usaideasttimor.net, lacked a privacy notice link on the 'Contact Us' page. It is noted this is the only page on which data can be entered.

- **Domain Registry** – Of the eight websites reviewed, the following six websites are listed on non-.gov domains:
  - http://www.eehicd.net;
  - http://www.usaidkenya.org;
  - http://www.usaidjordan.org;
  - http://ane-environment.net;
  - http://www.usaideasttimor.net;
  - http://www.usaidafghanistan.org.

  However, the following four websites also exist on the .gov domain:
  - http://www.usaidkenya.org;
  - http://www.usaidjordan.org;
  - http://www.usaideasttimor.net;
  - http://www.usaidafghanistan.org.

However, when trying to access the http://kenya.usaid.gov website, located on the .gov domain, the website does not allow a connection to be established.

The ADS 557 states the following, "In accordance with the OMB Memorandum 05-04, "Policies for Federal Agency Public Websites," as of December 31, 2005, web pages containing official U.S. Government information or which conduct transactions or other business related actions on behalf of the Agency must reside on .gov domains."

The lack of monitoring of Agency funded websites coupled with existent configurations on the web servers may result in the unintentional disclosure of information by web site users or USAID employees.

On June 8, 2006, the Office of Inspector General issued "Audit of USAID's Implementation of Key Components of a Privacy Program for its Information Technology Systems" (Report No. A-000-06-003-P). The report identified that USAID had not established and implemented a formal process to monitor agency funded websites to ensure the privacy of website users was protected. Since this

issue had been addressed during the OIG Privacy audit, we are not making a recommendation in this area.

However, we are making the following recommendation:

Recommendation No.4

We recommend that USAID's Chief Privacy Officer, in collaboration with Bureau for Legislative and Public Affairs/Public Information, Production and Online Services, assemble a complete inventory of USAID funded websites.

5. USAID had not prepared a report of its use of information in an identifiable form along with its privacy and data protection policies and procedures.

§522 of the Consolidated Appropriations Act of 2005 requires each agency to prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report is required to be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. However, USAID has not prepared a report of its use of information in an identifiable form along with its privacy and data protection policies and procedures because the Agency has recently appointed a Chief Privacy Officer to ensure that privacy laws and regulations are adhered to.

The Agency's Inspector General provides oversight to ensure that USAID is in compliance with Federal requirements. Without a written report, it is difficult for the Inspector General to assess the status of the privacy program and ensure that requirements of §522 are met.

Recommendation No.5

We recommend USAID's Chief Privacy Officer complete the report of USAID's use of information in an identifiable form and record it with the Agency's Inspector General.

6. USAID had not implemented role-based training for individuals responsible for personally identifiable information.

The ADS 545 Conforming Amendments requires that the Agency establish and provide annual Privacy Awareness training to all staff that use PII in routine performance of their duties. For individuals who have additional responsibility for PII, the Agency must provide role-based training. USAID has incorporated privacy related tips into their "Tips of the Day" security awareness program. However, role-based training has not been implemented for individuals responsible for PII. In addition, specific user roles have not been identified to receive role-based training. According to USAID officials, these roles will be outlined in the new ADS 508 and training will coincide with the release of ADS Chapter 508 and the new release of Tips of the Day.

Without proper privacy training, users may not be properly informed of the importance of information they handle and the legal and business reasons for maintaining its integrity and confidentiality.

Recommendation No.6

We recommend that USAID's Chief Privacy Officer identify specific user roles requiring role-based training and develop and implement an agency-wide training program regarding role based training for individuals responsible for personally identifiable information.