USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF SELECTED APPLICATION CONTROLS OVER THE ANNUAL REPORT APPLICATION SYSTEM

AUDIT REPORT NO. A-000-06-005-P
September 27, 2006

WASHINGTON, DC

Office of Inspector General

September 27, 2006

MEMORANDUM

TO: PPC/DAA, Walter North
M/DCIO, Phil Heneghan

FROM: AIG/A, Joseph Farinella /s/

SUBJECT: Audit of Selected Application Controls over the Annual Report Application System (Report No. A-000-06-005-P)

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

This report contains seven recommendations to help USAID improve its controls over the Annual Report Application system. Based on your comments to our draft report, we consider that management decisions have been reached for Recommendation Nos. 1, 2, 3, 4, 5, 6, and 7. For these recommendations, please notify the Bureau for Management's Audit, Performance and Compliance Division when final action is completed.

I want to express my sincere appreciation for the cooperation and courtesy extended to my staff during the 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. conducted this audit to review selected application controls[1] over the Annual Report (AR) Application system. The Bureau for Policy and Program Coordination (PPC) within USAID, developed, maintained and operated the Annual Report (AR) Application system with contractor support. (See pages 3 and 12.)

The audit found that USAID did not implement effective application controls for the AR system. Specifically, USAID did not:

- Perform risk assessments to identify the initial types of controls needed for the AR system or conduct follow-up annual assessments to monitor the effectiveness of existing controls (pages 4-5);
- Prepare a security plan that documents the needed (i.e., agreed-upon) controls in the AR system to mitigate risk in conformance with the National Institute of Standards and Technology guidelines (pages 5-7); and
- Implement selected controls, including effective password access controls, as necessitated by Federal requirements (pages 7-8).

These key deficiencies contributed to numerous other control weaknesses, such as not assigning security responsibilities, requiring training for users prior to obtaining access to the AR system, and testing contingency plans. Consequently, USAID has limited assurance that the AR's system controls are effectively mitigating risks of unauthorized disclosure, modification, destruction or loss.

The primary cause for these weaknesses was that the Cognizant Technical Officer (CTO) within the Bureau for Policy and Program Coordination (PPC) did not monitor the contractor's performance to ensure that the security requirements were performed and that the CTO did not obtain the specialized training needed to support their security responsibilities. More importantly, the Chief Information Officer's (CIO) office did not fully implement its oversight responsibility of monitoring the AR system to ensure that an acceptable level of security was established. (See pages 4, 8-9.)

We made seven recommendations to help USAID improve application controls over the AR system. (See pages 9-10.)

USAID management agreed to take corrective action on all seven recommendations in the report. Based on management's response, management decisions were reached on all seven recommendations. (See page 11.)

[1] Application controls are security controls that provide safeguards to protect the computer system and its information.

BACKGROUND

The United States Agency for International Development (USAID), Bureau for Policy and Program Coordination (PPC), developed, maintained and operated the Annual Report (AR) Application system with contractor support.[2] The AR system supports USAID reporting needs by collecting and analyzing program and resource information from worldwide operating units. First deployed in fiscal year (FY) 2002, the AR system evolved from the Review, Results, Resource, Request (R4) preparation tool to its present use. The AR system has since become critical for the support of budget and performance reporting requirements and is the primary means for obtaining program reporting documentation for the Agency.

The AR system supports the preparation of:

- USAID's Congressional Budget Justification (CBJ)
- USAID's Performance and Accountability Report (PAR)
- USAID's Annual Budget Submission
- Joint Department of State/USAID's Performance Plan
- USAID's Bureau Program and Budget Submission
- Office of Management and Budget's Performance Assessment Rating Tool
- USAID's Workforce Planning Request Levels

The AR system also maps expenditures to strategic objectives in the Statement of Net Costs. The changes to the AR system now being proposed include using the system to collect the use of 39 standardized program components[3] to support USAID's strategic planning process.

The AR system is predominantly housed, maintained and operated by an off-site contractor. (See Appendix III for a description of the system.)

Several legislative and policy-directed mandates define the types of controls that USAID computer systems should have. These mandates include:

- The Federal Information Security Management Act of 2002 (FISMA), which requires the National Institute for Standards and Technology (NIST) to develop standards and guidelines for information systems used or operated by an agency or by a contractor for an agency or on behalf of an agency; and gives the Office of Management and Budget (OMB) responsibility to oversee and coordinate the development and implementation of NIST standards and guidelines for Federal agencies.

- The OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" (November 28, 2000), which establishes

[2] Contract Number RAN-C-00-03-00032-00, awarded on August 1, 2003, contains a base year and two option years. The second option year expires on July 31, 2006.

[3] Program components are the "building blocks" of USAID programs. They will be standard across all Operating Units and have associated with them a set of common indicators to facilitate performance management and reporting.

minimum controls to ensure that adequate security is provided for the agency's computer systems.

- The USAID Automated Directives System (ADS), Chapter 545 - Information Systems Security, which contains specific mandatory security policies in support of FISMA, OMB and NIST mandates.

At the start of this audit, PPC organizationally was the system owner of the AR system. Subsequent to our audit field work, we learned that some components of the AR system will be replaced[4] by an integrated system to support the Department of State's Office of the Director of U.S. Foreign Assistance (F). Several USAID PPC personnel who had supported the AR system have been moved into the F bureau to assist in integrating USAID's AR system and the Department of State's Country Operational Planning and Reporting System. As a result of these changes, the recommendations made in this report should also be considered when implementing the new system.

AUDIT OBJECTIVE

This audit was added to the OIG's annual audit plan to answer the following question:

Did USAID implement effective application controls for the Annual Report (AR) Application system?

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

[4] The components for replacement or integration are planned to be identified and evaluated in the remaining part of calendar year 2006.

AUDIT FINDINGS

Although USAID through its contractor implemented some security controls, it did not implement effective application controls for the Annual Report (AR) Application system. Among the controls USAID's contractor did implement were physical access restrictions to their computer room, the performance of data backups of the AR system, and the development of limited edit checks and password control capabilities within the AR system. USAID also developed security policies and procedures to support information technology acquisitions and conducted ad hoc training for AR system users.

However, USAID did not implement effective application controls for the AR system. As described below, USAID did not (1) perform risk assessments; (2) prepare a security plan which may include identifying the AR system as a major application; and (3) implement selected controls, including effective password controls, as mandated by Federal requirements.

The risk assessment, security plan, and passwords are critical key controls that serve not only to support other application control categories (i.e., audit and accountability controls), but also to define and manage the risks of the AR system and the information it contains.

USAID Did Not Implement Effective Application Controls for the AR System

Summary – USAID did not implement effective application controls for the AR system. Specifically, USAID did not (1) perform risk assessments, (2) prepare a security plan, and (3) implement selected controls, including effective passwords, in accordance with the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB) and USAID requirements. This occurred because the Office of Policy and Program Coordination (PPC)—the system owner— (1) did not monitor the contractor's performance to ensure that the security requirements were performed and (2) obtain for the Cognizant Technical Officer (CTO) the specialized training needed to define and support their security responsibilities. In addition, USAID's Chief Information Security Officer did not conduct oversight reviews to re-evaluate the system as it evolved and ensure that minimum security requirements existed for the AR system. Consequently, USAID places the confidentiality, integrity and availability of the AR system and data at risk of unauthorized disclosures, modifications, destruction or loss.

Risk assessments are needed for the AR system - The purpose of an initial risk assessment is to identify risks to the computer system and the information contained in it so that appropriate controls can be defined and implemented to reduce or eliminate those risks to an acceptable level. Performing subsequent assessments helps ensure that controls are working as intended. Federal agencies that utilize contractors to install and/or maintain computer systems are fully responsible and accountable for ensuring that FISMA and related policy requirements are implemented, reviewed, and included in the terms of the contract.

- FISMA (section 3544) requires Federal agencies to conduct periodic assessments of all systems, including systems and information managed by a contractor on behalf of the agency, at least annually.

- USAID's policy ADS 545.3.1.4 Risk Management states that the individual responsible for daily and operational management of each specific system must (1) conduct an initial risk assessment for each information system using USAID published procedures and guidelines, (2) conduct follow-up risk assessments annually, or whenever the system or its operating environment significantly changes; and (3) take corrective actions to mitigate vulnerabilities detected during risk assessments.

However, PPC (the system owner) did not conduct risk assessments in accordance with FISMA requirements and USAID policy. Specifically, the Cognizant Technical Officer (CTO) responsible for monitoring the contract did not ensure that initial and subsequent annual assessments of the AR system were performed and appropriately documented. Further, the CTO was not fully aware of FISMA and USAID requirements to perform risk assessments. (This is discussed in more detail in the "Causes and Impacts of Problems Identified" section of the report.)

A system security plan is needed for the AR system – A system security plan (Plan) is a formal document that provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements. The Plan defines the agreed-upon controls that the AR system should have to mitigate risks.

OMB Circular A-130, Appendix III, requires Federal agencies to develop security plans consistent with NIST Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems," which states in part that all information systems must be covered by a system security plan.

Further, to develop a security plan, the system owners, in collaboration with the Chief Information Security Officer (CISO), must decide if the AR system is covered as a "major application" or a "general support system." OMB Circular A-130, Appendix III, defines a "major application" as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. The Circular also defines the term "major information system" as an information system that requires special management attention because of its importance to an agency mission or its significant role in the administration of agency programs, finances, property, or other resources. OMB defines a general support system as a system that consists of hardware and software to provide general data processing and telecommunication support for a number of applications (e.g., the local area network).

However, as discussed in the following sections, USAID did not (1) develop a security plan for the AR system in accordance with *FISMA, NIST and OMB* requirements and (2) consider identifying the AR system as a major application.

The AR system security plan was not developed – *ADS 545* gives the system owners the responsibility for (1) ensuring that a security plan is prepared, (2) implementing the plan, and (3) monitoring its effectiveness. Further, OMB directs agencies to develop security plans that address the following:

- Rules of behavior
- Security training
- Personnel screening
- Continuity of support or contingency planning
- Technical security controls
- Review of controls, and
- Authorization of Processing

However, USAID did not have a security plan for the AR system. Specifically, although the contract required the contractor to develop a system security plan in accordance with NIST 800-18, the CTO responsible for monitoring performance of the contract did not ensure that a Plan was developed for the AR system. (This is discussed in more detail in the "Causes and Impacts of Problems Identified" section of the report.)

The AR System Plan may need to identify the system as a major application – As previously stated OMB defines the term "major application system" as an information system that requires special management attention because of its significant role in the administration of agency programs, finances, property, or other resources. NIST 800-18 further states that "major applications" are by definition "major information systems" and must have a moderate to high impact level on the agency.

In its fiscal year 2005 FISMA report, USAID did not list the AR system as a "major information system." As such, USAID considered the AR system as a non-major or minor application system that runs on the general support system. However in accordance with OMB Circular A-130 and NIST guidelines, we believe that the AR system may meet the criteria for a "major application."

For example, various factors—including the high visibility of the AR system process, the criticality of its functions, and its use as a tool to prepare, among other documents, the Congressional Budget Justification and the Agency's resource requests—warrant, we believe, special management attention to the system's security as required by OMB Circular A-130. To illustrate:

- USAID's PPC acknowledges the importance of the AR system by stating in their FY2006 annual guidance:

> "The Annual Report application has become the Agency's primary program reporting document; it is critically important for a number of budget and performance reporting requirements. In addition, the Annual Report application is one of the tools of the Agency's strategic management reform and as such serves as the operational plan for all units. Due to the importance of the information collected in the Annual Report, PPC will advise senior management of all Missions that fail to fully meet the requirements herein**.**"

- USAID's PPC officials stated that without the AR system, these functions could not readily be performed using spreadsheets and word processing programs and to do so would be time consuming, laborious and produce results of questionable accuracy. Furthermore, PPC officials questioned whether such an option could be supported with existing staff resources. Information provided by, and stored in, the AR system is critical for USAID to request funding and carry out planning and budgeting. One PPC official indicated that USAID operations would cease if the AR system became unavailable since there was no alternative to preparing USAID's Congressional Budget Justification.

- USAID's geographic and functional bureaus currently use the AR system for preparing the Agency's Congressional Budget Justification and for their program planning and budgeting. In addition, the Office of Financial Management uses the system data for its Statement of Net Costs and for mapping USAID expenditures to its strategic objectives. USAID's increased use and reliance upon the system has made it critical to Agency operations.

- Lastly, the OIG's limited impact assessment concluded that the AR system's rating is at least "moderate." This means that the potential impact on USAID, should certain events occur, would be to jeopardize the information and information systems needed by the Agency to accomplish its assigned mission, protect its assets, and maintain its day-to-day functions. This impact level is consistent with NIST Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Systems;* NIST 800-18, which requires major applications to have a moderate to high impact rating; and NIST 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* which correlates information to predefined impact levels.

In our opinion, USAID's use of and reliance on the AR system appears to meet OMB's definition of a major application. The reports produced by the AR system and the information contained within it could only be produced with increased investment, time and effort. The loss of this system could be detrimental to Agency operations. Therefore, we believe that USAID should consider identifying the AR system as a major application.

Implementation of security controls needed – NIST 800-18 requires agencies to clearly identify their security controls and include a description of the considerations made for implementing security controls. Additionally, OMB A-130 Appendix III directs agencies to develop security plans that address specific security controls. The table on the next page depicts selected OMB A-130 Appendix III security controls and our assessment as to whether these controls were implemented for the AR system.

OMB A-130 Appendix III – Selected Controls Required in Security Plan	Implemented for AR System?
Has security been assigned to a management official knowledgeable of the information and processes supported by the application?	No
Have rules been established concerning use and behavior of individuals with access to the application to provide security to the application and information in it?	No
Did users receive specialized training focused on their responsibilities and application rules prior to receiving access to the application?	No
Have separation of duties, along with least privilege and individual accountability controls, been incorporated into the application and application rules?	Partially
Has contingency planning and periodic testing of the application been performed?	No
Have independent reviews or audits of the security controls been performed at least every 3 years?	No
Has a management official authorized in writing the use of the application by confirming that its security plan as implemented adequately secures the application and reauthorizes its use at least every 3 years?	No

As illustrated in the table above, USAID did not (1) assign a systems security officer to the AR system, (2) ensure that formal rules of behavior and specialized training were provided prior to an AR system user being granted access to the AR system, (3) conduct periodic contingency testing of the AR system, (4) conduct independent reviews or audits of the security controls, and (5) authorize the use of the AR system. In addition, although USAID partially implemented the capability to separate end-users and super-user privileges into the AR system by user identifications and passwords as explained below, PPC did not effectively implement passwords controls.

Effective password controls needed – OMB A-130 Appendix III, states that agencies are required to establish controls to ensure adequate security. For example, authentication of individual users is an important management control, for which password protection is a control mechanism. However, password protection will only be effective if a strong technology is employed and managed to ensure that it is used correctly. USAID's ADS 545.3.3.1, Identification and Authentication (Passwords) requires the use of password standards and procedures.

Nevertheless, contrary to ADS policy, USAID did not use effective password controls. For example:

- Passwords were not always required.
- Passwords had no expiration dates.
- Passwords had no requirement for complex construction.
- Passwords were not masked or hidden when signing in.
- The super-users who administer user accounts could view all users' passwords within their own bureaus because the passwords were not encrypted.
- Some accounts had blank passwords on the database server.[5]

[5] The Database Administrator promptly corrected this situation during the audit.

Causes and Impacts of Problems Identified – This audit identified a number of control weaknesses related to the AR system. We attribute these weaknesses to the CTO's need to:

1. exercise more active monitoring of the contractors to ensure that they are performing their security tasks and safeguarding the AR system, and
2. obtain specialized training that focuses on defining and supporting security responsibilities.

More importantly, the CISO in the Chief Information Officer's (CIO) office needs to fully implement his oversight responsibilities to ensure that an acceptable level of security is established for the AR system.

The contract supporting the AR system operations, awarded in August 2003, required the contractor to comply with OMB A-130, NIST Special Publication 800-18, and ADS 545, "Information Systems Security." All of these guidelines and USAID policies call for conducting risk assessments, preparing security plans, and implementing security controls for systems. However, USAID did not implement the guidelines and its own policies to protect the AR system. Specifically, the CTO did not monitor the contractor to ensure that the cited requirements were done. This, in part, was due to the CTO not being fully aware of the security requirements that should be implemented. Prior to speaking with us, the CTO did not know that risk assessments or security plans with implemented or planned controls were needed for the AR system. She indicated that she had not received the specialized training for employees with significant security responsibilities, which is required by FISMA.

In addition, ADS 545 states that the CISO must verify that the security level has been correctly established for each USAID information system. ADS 545 also states that the CISO must validate for each USAID information system that the appropriate managerial, operational and technical controls have been selected and implemented by the system owners. Although the CISO office staff conducted earlier reviews of the AR system, the CISO did not continue to monitor the system as it evolved to ensure that an acceptable level of security existed and that appropriate controls were implemented.

Without conducting initial and annual risk assessments, ensuring the AR system is covered by a system security plan, and ensuring effective passwords, the Agency has limited assurance that the AR system controls are appropriately addressing the risks and are functioning as intended. Consequently, the confidentiality, integrity and availability of the AR system and data are at risk and may not be protected from unauthorized disclosures, modifications, destruction and loss.

Subsequent to our fieldwork, we learned that some components of USAID's AR system will eventually be phased out and replaced[6] by an integrated Department of State and USAID system to support the Office of the Director of US Foreign Assistance (F) within the Department of State. The types of system controls mentioned in this report should be considered in F bureau's efforts in developing a new joint integrated system. Therefore, we are making several recommendations to help USAID improve its controls over the AR system.

[6]The components for replacement or integration are planned to be identified and evaluated in the remaining part of calendar year 2006.

Recommendation No. 1: We recommend that the Office of Policy and Program Coordination, in collaboration with the Chief Information Security Officer, re-evaluate the categorization of the Annual Report system and determine if it should be considered a major application system as defined by the Office of Management and Budget and the National Institute of Standards and Technology.

Recommendation No. 2: We recommend that the Office of Policy and Program Coordination, in collaboration with the Chief Information Security Officer, ensure that the Annual Report system is covered by a security plan as appropriate for the categorization of the Annual Report system.

Recommendation No. 3: We recommend that the Office of Policy and Program Coordination, in collaboration with the Chief Information Security Officer, ensure that a risk assessment of the Annual Report system is performed in conformance with the National Institute of Standards and Technology guidance to assist in categorizing and identifying the appropriate level of system controls for the Annual Report system.

Recommendation No. 4: We recommend that the Office of Policy and Program Coordination implement the appropriate controls to protect the Annual Report system. At a minimum, the security plan covering the Annual Report system controls should include:

- *Assigning security responsibilities.*
- *Establishing formal rules of behavior and providing training prior to a user being granted access to the Annual Report system.*
- *Conducting periodic contingency testing of the Annual Report system.*
- *Conducting independent reviews or audits of the security controls.*
- *Authorizing the Annual Report system for processing (if appropriate).*

Recommendation No. 5: We recommend that the Office of Policy and Program Coordination implement improved password controls over the Annual Report system in accordance with Automated Directives System-545 standards.

Recommendation No. 6: We recommend that the Office of Policy and Program Coordination provide the Cognizant Technical Officer for the Annual Report system specialized information systems security training to help ensure that information systems security deliverables are appropriately defined, evaluated and monitored for performance.

Recommendation No. 7: We recommend that the Chief Information Security Officer conduct a review of his oversight responsibilities and implement identified improvements to ensure that the Annual Report system has continued compliance with applicable Federal requirements.

EVALUATION OF MANAGEMENT COMMENTS

USAID's Deputy Assistant Administrator for the Office of Policy and Program Coordination (PPC) and the Acting Chief Information Officer (CIO) prepared a consolidated written response to our draft report. The consolidated response is included in its entirety in Appendix II of this report.

USAID management agreed to take corrective action on all seven recommendations in the report. For Recommendation Nos. 1, 2, 3, 4, 6, and 7, USAID management provided corrective action plans and target completion dates. Additionally, a management decision was made for Recommendation No. 5 and documentation is pending for final action. Therefore, we consider that management decisions have been reached for the above recommendations.

SCOPE AND METHODOLOGY

Scope

The Office of Inspector General, Information Technology and Special Audits Division, performed this audit in accordance with generally accepted government auditing standards. The purpose of the audit was to determine whether USAID implemented effective controls over its Annual Report (AR) Application system. Audit fieldwork was conducted at USAID headquarters in Washington, D.C. and at the offices of the LTS Corporation in the Washington, D.C. metropolitan area from November 29, 2005, through April 17, 2006. Our scope also included input from AR system users in overseas operating units.

In support of our audit objective, we selectively considered the following areas, among others, in our review:

- Risk Assessments and Security Plans
- Access Controls
- Audit Trials
- Contingency Planning
- Training

Though several contracting issues were identified during the audit, an audit of the terms of the contract was outside the scope of this audit.

Methodology

For the purpose of this audit, application controls were defined as security controls that provide management, technical and operational safeguards to protect the confidentiality, integrity and availability of the system and its information. As a basis for our evaluation, we relied primarily upon the National Institute for Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," as the framework for identifying the types of controls to be included in our audit. We also used the Office of Management and Budget (OMB) Circular A-130, the Federal Information Security Management Act of 2002 and guidance issued by the Institute of Internal Auditors, Information Systems Audit and Control Association, Defense Information Systems Agency, NIST Federal Information Processing Standards Publication 199, and other NIST publications.

We interviewed direct-hires and contractors from USAID's Office of Program and Policy Coordination, Bureau for Asia and Near East, Bureau for Africa, and the Office of Information Resources Management. In addition, we obtained input from USAID's overseas missions through the use of a questionnaire.

As noted above, a survey of USAID's overseas missions on the AR system was made through a questionnaire sent to 66 AR system users in 15 different countries. Twenty-two of the 66 individuals responded. This list of AR system overseas mission users was provided by the contractor that supports the AR system. The purpose of the survey

questionnaire was to determine how these operating units managed access to and use of the application.

We reviewed relevant laws, regulations, leading practices, and USAID policies, procedures, and guidance. We also reviewed the Agency contract regarding the AR system and results of other audits and reviews related to our audit objective. In instances where documentation was not available to test, verify or support a specific security control area, we used the responses received from Agency and Contractor personnel as a basis for determining the security control's effectiveness. Additionally, we conducted a preliminary evaluation of the AR system to determine whether the AR system could be categorized in a security plan as a major application using criteria established in NIST's Federal Information Publication Standard 199, supporting Special Publications 800-18, 800-37, 800-53, 800-60 and OMB Circular A-130.

Using the above information, we identified and reported on selected security areas that we perceived as high risk based on the significance and sensitivity of that process, the likelihood that the particular process may not achieve its intended control objective, and the reliance of a particular process that supports other processes. Consequently, not all the security areas we reviewed are mentioned in the report.

A specific materiality threshold was not set for the audit. Instead, we used our judgment in determining sampling sizes to assess the AR system since the population was too small for statistical sampling.

MANAGEMENT COMMENTS

September 22, 2006

MEMORANDUM

TO: AIG/A, Joseph Farinella

FROM: PPC/DAA, Walter North /s/
CIO/A, Phil Heneghan /s/

SUBJECT: Audit of Selected Application Controls over the Annual Report Application (AR) System, dated August 24, 2006
IG Report No. A-000-06-00X-P

Thank you for your report. Below are our management decisions for the seven recommendations in the report.

Recommendation No. 1: Re-evaluate the Annual Report (AR) system and determine if it is a major application system.

Management Decision: PPC will conduct an evaluation of the AR system and make a determination whether it is a major application by July 2007.

Recommendation No. 2: The AR system must have an appropriate security plan.

Management Decision: PPC will develop a security plan for the AR system by July 2007.

Recommendation No. 3: A risk assessment of the AR system should be performed to identify the appropriate level of system controls.

Management Decision: PPC will conduct a risk assessment for the AR system by July 2007.

Recommendation No. 4: At a minimum, the IG recommends that certain AR system controls be included in the security plan.

Management Decision: PPC will follow the new CISO guidance (to be issued by March 2007) to identify the system controls to be included in the security plan for the AR system by July 2007.

Recommendation No. 5: Implement improved password controls.

Management Decision: PPC has already implemented improved password controls in accordance with ADS-545 standards.

Recommendation No. 6: The CTO for the AR system should receive information systems security training to ensure that information systems security deliverables are defined, evaluated and monitored for performance.

Management Decision: PPC will complete this training on or before November 30, 2006.

Recommendation No. 7: We recommend that the Chief Information Security Officer conduct a review of his oversight responsibilities and implement identified improvements to ensure that the AR system has continued compliance with the Federal requirements.

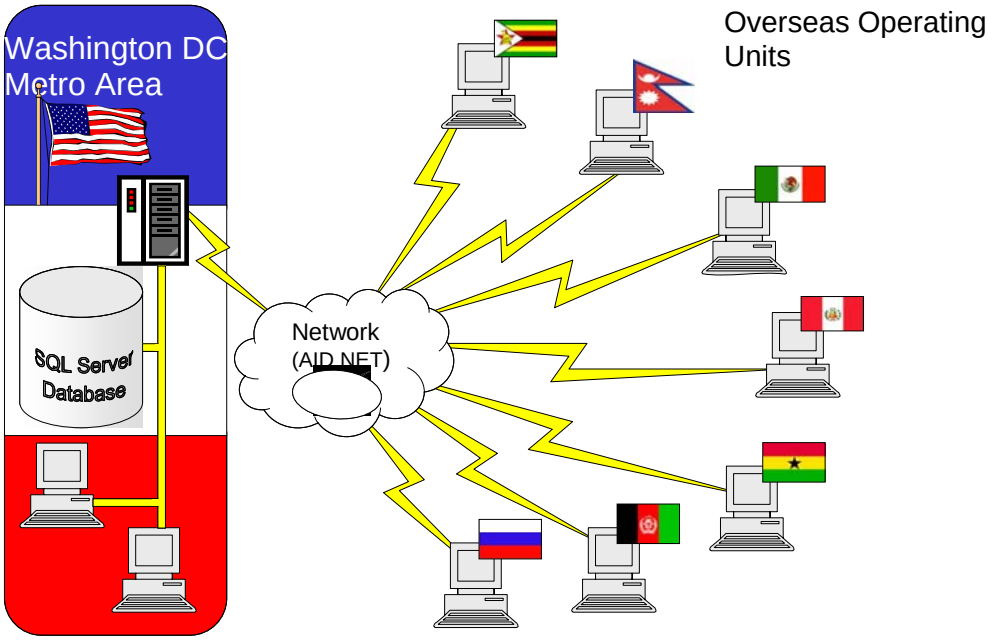
Management Decision: The CISO will conduct a review of oversight responsibilities related to the AR system and an establish procedures to implement identified improvements by July 2007.

Annual Reporting System Description

For each fiscal year, various additions and modifications are made to the Annual Report (AR) Application system by the Office of Policy and Program Coordination (PPC), with contractor support, to meet the Agency's reporting information needs and requirements driven by legislation and other Federal mandates and initiatives. The information collection process starts with the issuance of the AR guidance and an electronic distribution of the AR system software to Agency operating units by PPC and the Bureau for Legislative and Public Affairs. The AR guidance covers a broad range of budget data, performance data, and narrative topics to be collected for the Agency's various internal and external stakeholders. The Agency's overseas operating units receive and install the AR system software for users at their site. There they prepare and submit their information through the AR system back to Washington, DC, over USAID's network (AIDNet). In Washington, each operating unit's submission is stored in a core database system for the Regional Bureaus to access, review, analyze, and modify before the data is officially submitted to PPC. When the AR information is officially finalized, PPC extracts information from the AR system in coordination with other Agency offices to prepare internal and external reports (e.g. Performance and Accountability Report (PAR) and Congressional Budget Justification (CBJ)). This process is repeated annually and generally starts during the first quarter of each new fiscal year. However, the previous year's information is available within the system for review and inclusion in the current year's submission.

The AR system is a Microsoft Windows-based client server application[7]. As shown in the diagram on the next page, the core of the AR system is a central database that runs on Microsoft SQL Server software in a contractor-supported facility located in the Washington, DC metropolitan area. In conjunction with the core AR central database, an AR client application (i.e., a small database program using MS Access with a user interface) is installed on a user's computer to input, query and submit data. A dedicated communication line connects USAID Headquarters to the contractor facility, allowing Headquarters personnel with the AR client application to input and retrieve data from the AR central database. However, personnel in overseas operating units do not have direct access to the AR central database. Each overseas operating unit, upon local completion and approval of their input into the local AR client application, transmits its consolidated AR client application database back to Headquarters over the Ageny's network (AIDNet) and through a dedicated communication line for electronic storage at the contractor's facility. Around mid-December, PPC, with contractor support, imports the AR client application databases from each operating unit into the core AR central database where it is accessed by Headquarters personnel. The AR system does not directly receive information from any other Agency system. The diagram below represents a high-level pictorial representation of the AR system.

[7]Client-server application: Describes the relationship between two computer programs in which one program, the client, makes a request from another program, the server, which fulfills the request and provides a convenient way to interconnect programs that are distributed across different locations.


Washington DC
Metro Area
SQL Server
Database
Network
(AID NET)
Overseas Operating
Units

Glossary of Selected Information Security Terms

Access Control –	The process of granting or denying specific requests (1) to obtain and use information and related information processing services and (2) to enter specific physical facilities.
Accountability –	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Application –	The use of information resources (information and information technology) to satisfy a specific set of user requirements.
Availability –	Ensuring timely and reliable access to and use of information.
Audit –	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Authentication –	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Confidentiality –	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Information System Owner –	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Identification –	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
Impact –	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Integrity –	Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.
Risk Assessment –	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analysis.
Security Controls –	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
System Security Plan –	Formal document that provides an overview of the security requirement for the information system and describes the security controls in place or planned for meeting those requirements.

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