USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF APPLICATION CONTROLS FOR USAID/GLOBAL HEALTH BUREAU'S FIELD SUPPORT-AID SYSTEM

AUDIT REPORT NO. A-000-08-003-P
January 28, 2008

WASHINGTON, DC

Office of Inspector General

January 28, 2008

MEMORANDUM

TO: Senior Deputy Assistant Administrator, GH/AA, Gloria Steele

FROM: AIG/A, Joseph Farinella /s/

SUBJECT: Audit of Application Controls for USAID/Global Health Bureau's Field Support-AID System (Report No. A-000-08-003-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 in Appendix II.

This report contains two recommendations. The first is to help USAID improve application controls for its Field Support-AID system. The second recommendation addresses unneeded roles to USAID's core accounting system. Based on your response and the supporting documentation that you provided with your comments, final action has been taken on both recommendations.

I appreciate the cooperation and courtesies extended to my staff during this audit.

cc: Controller GH/SPBO, Kristine Smathers

CONTENTS

SUMMARY OF RESULTS

Information technology application controls are fully automated controls designed to ensure complete and accurate processing of data. Application controls vary based on the business purpose of the specific application and help ensure the privacy and security of data transmitted between applications. (Page 2.) The Information Technology and Special Audits Division of the Office of Inspector General conducted this audit to determine if USAID had implemented application controls for its Field Support-AID System to mitigate the risk of mismanaging appropriated funds. (Page 3.)

Overall, the audit determined that the application controls for the system were adequate, except that USAID did not formally document the approvals needed to access the system. For example, USAID implemented application controls that have certain edit checks built into the system to help ensure that data is accurate. However, the lack of proper approvals to access the system means that unauthorized users could gain access to sensitive information, thus increasing the risk of unauthorized use, loss, or modification of the information. (Pages 4-6.)

In addition, the audit found that the system administrator had unneeded roles in Phoenix (the Agency's core accounting system)[1]. Specifically, he had input capabilities to the system when he needed only view capabilities to perform his job. As a result, he had the ability to distribute and process funds for program and operating expenses, an ability which was incompatible with his job functions. (Pages 7-8.)

This report contains two recommendations. The first recommendation is to help USAID improve its application controls over the system (Page 6.) The second recommendation addresses the unneeded access to USAID's core accounting system. (Page 8.)

Based on USAID's response and the supporting documentation provided, final action has been taken on both recommendations. (Page 9.)

[1] This particular finding was not tied directly to our audit objective. However, during our fieldwork the issue was discovered and we felt it significant enough to report.

BACKGROUND

Information technology (IT) application controls are fully automated controls designed to ensure the complete and accurate processing of data, from input through output. These controls vary based on the business purpose of the specific application and help ensure the privacy and security of data transmitted between applications. Categories of IT application controls may include:

- Completeness checks - Controls to ensure that all records were processed from initiation to completion.
- Validity checks - Controls to ensure that only valid data are input or processed.
- Authentication - Controls to ensure that only authorized programs can read the data.

Field support is the process by which USAID missions “buy in” to centrally awarded contracts, cooperative agreements, and grants. For example, a mission may buy in to a grant for a broad range of environmental issues as they apply to regional security, stability, and conflict. This method can help meet the needs of USAID missions where (1) indefinite delivery contracts are not available, (2) contract staffing is insufficient in the field, or (3) a particular activity requires flexibility, and management of that activity more appropriately lies with the central bureaus. In fiscal year 2006, USAID missions obligated more than $400 million through field support agreements.

According to the system administrator, the field support process began in 1995, but the system used for tracking field support activity has changed over time. The system began with e-mail exchanges and spreadsheets, evolved to a basic database, and eventually to the current Web-enabled database system, called Field Support-AID (FS-AID).

In 2005 USAID interfaced FS-AID with Phoenix, USAID’s core accounting system. Although Phoenix tracks expenditures, it has no budgeting capabilities and does not contain sublevel expenditure categories. Thus, USAID bureaus[2] use the system to track budget activity for field support by inputting planning, receiving, obligating, and commitments data into the system. In addition, USAID uses information in the system for reports to Congress.

[2] A bureau is a major organization unit of USAID that reports to the Office of the Administrator. A bureau administers complex and diverse programs involving a designated geographic area; major policy, program and technical advisory services; or management and program support functions.

AUDIT OBJECTIVE

This audit was conducted to answer the following question:

> Did USAID implement application controls for its Field Support-AID system to mitigate the risk of mismanagement of appropriated funds?

A description of the audit's scope and methodology is contained in Appendix I.

AUDIT FINDING

USAID implemented application controls for its Field Support (FS)-AID system to mitigate the risk of mismanaging appropriated funds, but USAID did not formally document the approvals needed to access FS-AID.

Specifically, USAID implemented edit checks built to help ensure that data within the system is accurate. The controls included the following (among other things):

- Checks to ensure that the input field accepts the appropriate numeric format and the required number of characters. For example, for the “Commit/Amend” field, the system validates the amounts entered and field support requests selected.

- Completeness checks that identify missing data fields. For example, FS-AID verifies that Strategic Objective values are not missing.

- Error and warning messages to indicate the type of problem encountered. For example, when a commitment comes back from Phoenix as “Failed,” the system provides a screen where users can view the error messages returned. In addition, an event log records any error messages for processes that are not seen by the user. System administrators can check this log to troubleshoot any data errors and inconsistencies or unresponsiveness reported by users.

However, USAID did not formally document the approvals needed to access FS-AID. The following section discusses this issue in detail.

USAID Did Not Have Formal Documented Access Approval to FS-AID

Summary: USAID did not formally document approvals needed to access FS-AID, as required by National Institute of Standards and Technology Special Publication (NIST) 800-12. According to Agency personnel, the FS-AID policy and procedures manual, including the FS-AID Access Form, was never finalized. Because the FS-AID system did not have proper access approvals in place unauthorized users could gain access to the system and its sensitive information, thus increasing the risk of unauthorized use, loss, or modification of the information.

According to Section 10.2 of NIST 800-12, *An Introduction to Computer Security:*

> Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations.

According to NIST 800-12, authorization to access a system is granted, directly or indirectly, by the application or system owner.

In addition, according to the U.S. Government Accountability Office's (GAO) "Standards for Internal Control in the Federal Government:"

> Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

According to the system administrator, access to the FS-AID requires a "Rule of Two." Two members of USAID management must request access, stating the reason why access is needed and whether read or write access is appropriate. However, the system administrator also stated that there is no formal access authorization form. Instead, mission users are granted access to the system via e-mail requests. The system administrator stated that he generally (but not always) keeps e-mails pertaining to access by mission users. The system administrator does not require e-mail permission from USAID management for Washington users. Rather, the system administrator grants access after receiving verbal permission from either the individual requestor or the individual's supervisor.

Based on a random sample of 50 from a list of 596 users, 34 (68 percent) did not have documented access rights. Specifically, of the 34 users, 15 could enter data into the system and 19 had read only access.

According to the FS-AID system administrator, USAID management did not believe formal documented access was needed because (1) FS-AID is not a financial system and (2) the security set-up is a single sign-on application linked via USAID's network. However, although the aforementioned statement may be true, the FS-AID system contains sensitive information and is linked to Phoenix. Therefore, proper access approval procedures are needed in order to protect data within the system from unauthorized users.

Nonetheless, according to the draft "Access Control, Incident Response, and Security Risk Management Policies and Procedures" for FS-AID, to "obtain access to the FS-AID, an individual shall complete the FS-AID Access Form contained in the attached Adobe Acrobat File." However, USAID did not finalize and put that document into use. According to the system administrator, the document was drafted to demonstrate to the chief information security officer, Phoenix security team, and deputy chief financial officer that FS-AID had effective security control measures in place so as to obtain their approval for the interface between FS-AID and Phoenix to be activated. However, USAID officials decided to approve activation without that document. As such, an FS-AID Access Form was not prepared.

Because the FS-AID system did not have proper access authorization in place, unauthorized users could gain access to the system and its sensitive information, thus increasing the risk of unauthorized use, loss, or modification of the information. Although no instances of unauthorized access were identified, the system administrator determined that 9 of the 50 users (18 percent) in the sample no longer required access to the system. Thus, we are making the following recommendation:

> *Recommendation No. 1: We recommend that the Field Support-AID System Owner document the approval procedures that authorize access to the Field Support-AID system. At a minimum, these procedures should include the requirement for formal documentation of access rights, approvals, and periodic recertification.*

OTHER MATTERS OF INTEREST

Although this issue does not relate directly to the audit objective, it was identified during audit fieldwork and needs to be brought to the attention of USAID management for corrective action.

Field Support-AID System Administrator Has Unneeded Roles in Phoenix

Summary: Contrary to NIST 800-53, USAID's Field Support-AID system administrator has unneeded roles in Phoenix, USAID's core accounting system. This problem occurred because the system administrator was given these roles during the Phoenix overseas deployment. These unnecessary roles gave him the ability to distribute and process funds for program and operating expenses, an ability which was incompatible with his job functions.

According to appendix F of NIST Publication Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, the organization should establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

The FS-AID system administrator is responsible for developing, implementing, managing, and operating information systems for field support activity. In addition, he is responsible for providing technical leadership for data management tasks. However, based on a query of Phoenix, USAID's core accounting system, the system administrator has the ability to input information into Phoenix. Specifically, he was given roles that allowed him to:

- Distribute funds at the activity level for dollars appropriated for program and operating expense funds.

- Process the funds for program and operating expense.

According to the system administrator, those roles in Phoenix are not required to perform his job functions, which are to coordinate, facilitate, track and monitor commitments. He affirmed that he needs only read-only access to help him perform his duties.

According to the system administrator, he never used the aforementioned roles in Phoenix, and viewed information only to help him manage and track field support requests and commitments. Moreover, a query of Phoenix showed that the system administrator never processed transactions in Phoenix.

According to Phoenix Security officials, the FS-AID system administrator was given these additional roles in the event his assistance was needed to create mission budgets at the activity level during the Phoenix overseas deployment.

As a result, the system administrator had the ability to distribute and process funds for program and operating expenses, an ability which was incompatible with his job functions. Upon being informed of this, the system administrator initiated a request that those roles be removed. Nonetheless, we are making the following recommendation:

> *Recommendation No. 2: We recommend that the Controller in the Global Health Bureau's Office of Strategic Planning, Budget & Operations review the Field Support-AID system administrator's roles in Phoenix to determine which roles are needed for his current job functions and, based on the results of that review, make needed requests to the Phoenix Security team to modify those roles.*

EVALUATION OF MANAGEMENT COMMENTS

USAID management concurred with Recommendations No. 1 and No. 2. Based on the response and supporting documentation provided, final action was taken on Recommendation No. 1 and Recommendation No. 2 upon issuance of this report.

For Recommendation No. 1, we recommended that the Field Support-AID System Owner document the approval procedures needed to access the Field Support-AID system. At a minimum, these procedures should require formal documentation of access rights, approvals, and periodic recertification. In response, the Field Support-AID System Administrator Guide has been updated to require that (1) approval for access to the database be documented and (2) an annual review of all user accounts be conducted.

For Recommendation No. 2, we recommended that the controller in the Global Health Bureau's Office of Strategic Planning, Budget & Operations review the Field Support-AID system administrator's roles in Phoenix to determine which roles are needed for his current job functions and, based on the results of that review, make needed requests to the Phoenix Security team, to modify those roles. In response, the Bureau for Global Health and the Phoenix Security Team revised the Field Support-AID system administrator's roles accordingly, and limited his access to the system for only those roles necessary to carry out his job functions.

The complete text of USAID's management comments (excluding the attachment) is included in appendix II.

SCOPE AND METHODOLOGY

Scope

The Office of Inspector General (OIG), Information Technology and Special Audits Division, performed this audit in accordance with generally accepted government auditing standards. The purpose of this audit was to determine whether USAID implemented proper application controls for the Field Support-AID system to mitigate the risk of the mismanagement of appropriated funds. The reviews of application controls for this audit were limited to the following points:

- Data accuracy
- Completeness checks
- Validity checks of data
- Verifiability of data

Audit fieldwork was conducted at USAID headquarters in Washington, D.C, between May 17 and October 10, 2007.

Methodology

To answer the audit objective, we obtained and reviewed FS-AID documentation and conducted interviews with the FS-AID team. Specifically, we performed the following actions (among others):

- Assessed a sample of application controls against the National Institute of Standards and Technology Special Publications, U.S. Government Accountability Office's "Standards for Internal Control in the Federal Government," and the FS-AID System Design Document.
- Reviewed the overall process of the FS-AID application itself.
- Reviewed a random sample of users to determine if user access had been authorized. However, we performed only limited work to determine whether user privileges on the system were consistent with the documented user authorizations.
- Followed up on other OIG audit reports that addressed FS-AID and its controls, as appropriate.

We did not evaluate the field support process or assess the accuracy of the field support requests and commitments, nor did we not set a materiality threshold for this audit.

MANAGEMENT COMMENTS

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

FROM: GH/SPBO Controller, Kris Smathers /s/

SUBJECT: Bureau for Global Health's Response to the OIG's Draft Report Titled "Audit of Application Controls for USAID/Global Health Bureau's Field Support AID System" (A-000-08-00X-P)

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) Draft Report Titled "Audit of Application Controls for USAID/Global Health Bureau's Field Support AID System" (A-000-08-00X-P). The Bureau for Global Health (GH) has taken the following actions outlined below and is, therefore, requesting that the two recommendations be closed upon issuance of the OIG's final audit report.

Recommendation No. 1: We recommend that the Field Support-AID System Owner document the approval procedures for access authorization to the Field Support-AID system. At a minimum, these procedures should include the requirement for formal documentation of access rights, approval, and periodic re-certification.

GH concurs with the recommendation. The Field Support-AID System Administrator Guide has been updated to require (1) documented access approval for the database and (2) an annual review of all user accounts. Further, GH has designed and instituted an enhanced integrated electronic and paper record keeping system that will track and maintain supporting database access approval documentation for all new and re-certified user accounts. (Please see pages 4-1 and 4-10 in the attached revised FS-AID System Administrator Guide.)

On this basis, GH requests that the recommendation be closed upon issuance of the final audit report.

Recommendation No. 2: We recommend that the Controller of Operations in the Global Health Bureau's Office of Strategic Planning, Budget & Operations review the Field Support-AID system administrator's roles in Phoenix to determine which roles are needed for his current job functions and, based on that review, make needed requests to the Phoenix Security team for modifications of those roles.

GH concurs with the recommendation. The Bureau for Global Health has completed a review of the Field Support-AID system administrator's roles in Phoenix and determined that his current job functions require only the ability to make inquiries. In accordance with this review, the attached request was submitted to the Phoenix Security Team to revise the Field Support-AID system administrator's roles accordingly and the Phoenix Security Team has completed this modification in Phoenix.

On this basis, GH requests that the recommendation be closed upon issuance of the final audit report.

GH would like to thank the OIG staff for their thoughtful insights during the audit that we believe have resulted in improved controls for the Field Support AID System.

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