PD-ABU-875
113473

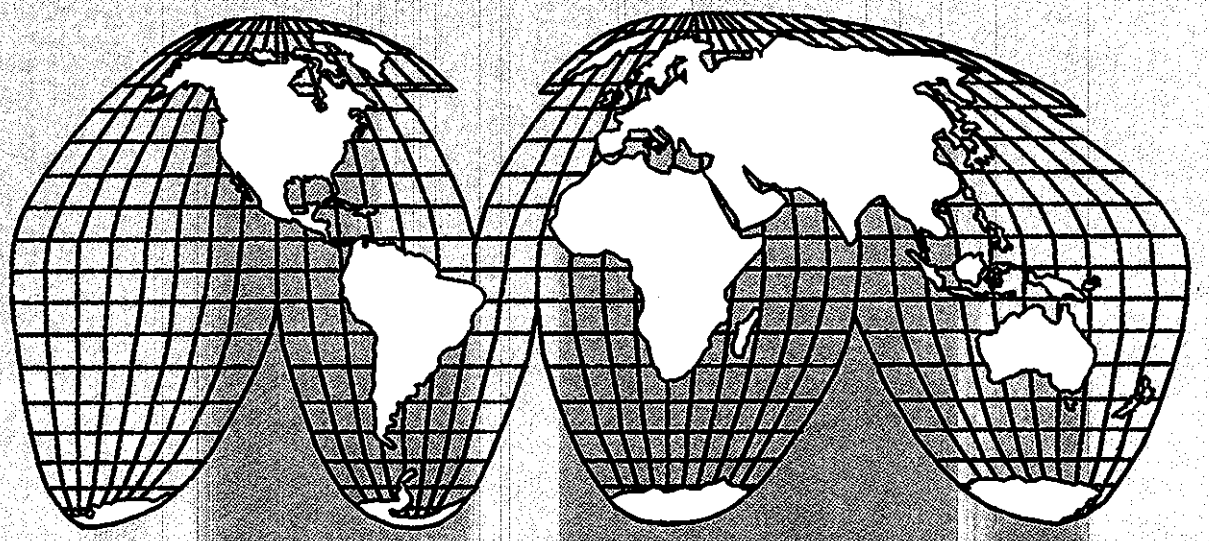
USAID

OFFICE OF INSPECTOR GENERAL

Audit of General Controls Over USAID/Bolivia's Mission Accounting and Control System

Audit Report No. 1-511-02-007-P

February 6, 2002



U.S. Agency for International Development
Regional Inspector General / San Salvador

A

U.S. Agency for
INTERNATIONAL
DEVELOPMENT

RIG/San Salvador

February 6, 2002

MEMORANDUM

FOR: USAID/Bolivia Director, Liliana Ayalde

FROM: Acting Regional Inspector General/San Salvador,
Steven H. Bernstein

SUBJECT: Audit of General Controls Over USAID/Bolivia's Mission Accounting and Control System (Report No. 1-511-02-007-P)

This memorandum is our report on the subject audit.

Management's comments on the draft report were considered in preparing this report. They are included for your reference in Appendix II.

This report includes five recommendations. A management decision has been made for Recommendation No. 1. The Office of Management Planning and Innovation will make a determination of final action after the recommendation has been completely implemented. Final actions have been taken on Recommendation Nos. 2 through 5 and will be closed upon issuance of the report.

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

Table of Contents

Summary of Results 3

Background 3

Audit Objective 4

Audit Findings 4

Did USAID/Bolivia's information system contain general controls to provide assurance that financial information reported was complete, reliable, and secured? 4

Logical Access Controls Need Strengthening 5

Contingency Plan Lacks Details 6

Assigned Duties not Appropriate 7

Management Comments and Our Evaluation 7

Appendix I – Scope and Methodology 8

Appendix II – Management Comments 10

Summary of Results

The Regional Inspector General/San Salvador conducted an audit to determine if USAID/Bolivia's financial information system contained general controls to provide assurance that information reported was complete, reliable, and secured (page 4).

USAID/Bolivia implemented general controls to provide assurance that financial information reported was complete, reliable, and secured. However, we noted areas where controls could be improved (page 4).

At USAID/Bolivia, general controls existed to safeguard financial data (page 4). Nevertheless, we found that access controls could be improved (page 5), that the contingency plan lacked details (page 6), and that the employee responsible for inputting access rights within the Mission Accounting and Control System (MACS) was also assigned key accounting duties. Being able to input access rights in MACS and having key accounting duties created a situation where management controls could be circumvented (page 7).

USAID/Bolivia agreed with the recommendations in this report, and management decisions have been made for the recommendations. The Office of Management Planning and Innovation will determine final action after Recommendation No. 1 has been implemented. Final actions have been taken on Recommendation Nos. 2 through 5 (page 7).

Background

General controls of an entity's information system are the structure, policies, and procedures that ensure the system's proper operation. The primary objectives of general controls are to safeguard data, protect computer application programs, prevent unauthorized access to system software, and ensure continued computer operations in case of unexpected interruptions.

USAID/Bolivia uses the Mission Accounting and Control System (MACS) to automate accounting and financial management functions. MACS provides financial information to USAID headquarters as well as to mission management and other interested parties. MACS is an on-line, interactive, fully integrated processing system in which data is updated continuously as transactions are posted. The system is designed to operate on Wang VS or Unix operating systems and is written in COBOL. The system at USAID/Bolivia operates on a server running the Unix operating system.

The users of MACS and its reports vary with the size of the mission and its accounting needs. In general, MACS users are the mission's accounting and voucher staff. MACS reports are used by the controller's office staff as well as by project officers, mission management, and executive office personnel.

USAID/Bolivia is the accounting station for the missions in Bolivia, Brazil, and Paraguay. According to USAID/Bolivia records, expenditures for fiscal year 2001 for those three missions, respectively, were $76,711,944; $4,162,756; and $4,686,102.

Audit Objective

The Regional Inspector General/San Salvador included an audit in its fiscal year 2002 audit plan to answer the following question:

> Did USAID/Bolivia's information system contain general controls to provide assurance that financial information reported was complete, reliable, and secured?

This audit focused only on the Mission Accounting and Control System (MACS). Appendix I describes the audit's scope and methodology.

Audit Findings

Did USAID/Bolivia's information system contain general controls to provide assurance that financial information reported was complete, reliable, and secured?

USAID/Bolivia implemented general controls to provide assurance that financial information reported was complete, reliable, and secured. However, in certain areas, controls could be improved. A management letter was delivered to USAID/Bolivia's mission director on February 6, 2002. That letter contained detailed, sensitive information on the weaknesses noted during the audit and is not included with this audit report.

The Computer Security Act (CSA) of 1987 requires federal agencies to establish information systems security plans and to provide periodic training for all persons that manage, use, or operate federal computer systems. Additionally, the Office of Management and Budget (OMB), in Appendix III to OMB Circular No. A-130, establishes a minimum set of controls to be included in federal information systems security programs.

Consistent with the requirements of the CSA and with Appendix III to OMB Circular No. A-130, USAID/Bolivia implemented the following general controls:

- Risks to information systems were assessed.
- A mission-wide security program was documented.
- A security structure with clearly assigned responsibilities was developed.

- Information resources were classified according to their criticality and sensitivity.

- A current list of authorized users and their authorized access was kept.

- Physical controls to prevent unauthorized access were established.

- Steps were taken to minimize potential damage and interruption in the event of an emergency.

The efforts of the mission staff in designing and administering these controls were commendable. Their commitment to information systems security was evidenced in the controls operating at the mission and was reflected in their conscientious attitudes.

Although the mission has implemented several effective controls, this report will now address areas that could be improved. Due to the existence of compensating controls that would prevent or detect material financial misstatements, none of the weaknesses explained below were "material weaknesses" as defined in Appendix I.

Logical Access Controls Need Strengthening

In addition to the CSA and to Appendix III to OMB Circular A-130, USAID policy dictates information systems security requirements. USAID policy states that access to systems and to specialized system software, utilities, and functionality on those systems must be protected. Software programs designed to prevent or detect unauthorized access are called "logical access controls."

USAID/Bolivia implemented logical access controls. Nevertheless, the following weaknesses with those logical access controls existed at the mission.

- User passwords did not comply with USAID password policies.

- Logs that record access attempts and logs that record the use of sensitive commands were not being reviewed.

- Controls were not implemented to prevent users from accessing system commands, programs, and data files.

The General Accounting Office (GAO) explained the possible consequences of inadequate access controls in the Federal Information System Controls Audit Manual (FISCAM). "Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data." By accessing data files, a user could obtain sensitive information or could make unauthorized changes for personal gain. By accessing application programs, a

user could modify how transactions are processed. For example, programs could be modified to process transactions that exceed available funding.

> **Recommendation No. 1: We recommend that USAID/Bolivia use a password management software program to enforce password policies.**
>
> **Recommendation No. 2: We recommend that USAID/Bolivia implement a procedure to review, on a regular basis, log files that detail access attempts and use of sensitive commands.**
>
> **Recommendation No. 3: We recommend that USAID/Bolivia restrict access to system commands and programs to system managers.**

Contingency Plan Lacks Details

Appendix III to OMB Circular No. A-130 directs agencies to establish and periodically test contingency plans. USAID policy specifies that these plans should contain "step-by-step instructions detailing remedial actions." Topics that should be included in a contingency plan are:

- supporting resources that will be needed,
- roles and responsibilities of those who will be involved in recovery activities,
- arrangements for off-site disaster recovery location,
- off-site storage location for backup files, and
- procedures for restoring critical applications.

USAID/Bolivia included these topics in its contingency plan except for procedures for restoring critical applications. Also, the plan did not include a section defining when and how the plan should be tested. The plan did not contain detailed recovery and testing procedures because systems management did not have guidance outlining the appropriate level of detail that should be included in a contingency plan.

Detailed recovery procedures are needed to minimize the recovery time in the event of a disaster and to allow others to recover the system if key information systems personnel are incapacitated in a disaster. Testing is essential to ensure that the contingency plan will work as designed.

Recommendation No. 4: We recommend that USAID/Bolivia include detailed recovery and testing procedures in its contingency plan.

Assigned Duties not Appropriate

USAID policy states that access privileges should be assigned consistent with users' functional responsibilities and authorities. According to FISCAM, "work responsibilities should be segregated so that one individual does not control all critical stages of a process." If duties are not segregated, the risk that errors will enter the system or that fraud will occur increases.

At USAID/Bolivia, the responsibility for inputting access rights to accounting, voucher examiner, and payment schedule approval functions within the Mission Accounting and Control System (MACS) was given to a key accounting employee. When the responsibility for inputting access rights was assigned to the accounting employee, USAID/Bolivia believed that the duty was consistent with the employee's overall job responsibilities. However, by having the ability to input access rights, the employee personally had the capability to perform any accounting, voucher examiner, or approval function. With unlimited access within MACS, the employee could have created projects, vendors, obligations, and commitments. The employee could have then scheduled vouchers for payment and certified them. Because the employee holds a key accounting position, the employee could have suppressed or manipulated information that would have exposed the unauthorized activity.

Although nothing came to our attention that would cause us to believe that the employee abused MACS security, the employee was in a position to influence accounting treatment while enjoying unlimited functional access in MACS.

Recommendation No. 5: We recommend that USAID/Bolivia assign the responsibilities for inputting access rights in the Mission Accounting and Control System to someone who does not have accounting duties.

Management Comments and Our Evaluation

USAID/Bolivia agreed with the recommendations in this report, and management decisions have been made for the recommendations. The Office of Management Planning and Innovation will determine final action after Recommendation No. 1 has been implemented. Final actions have been taken on Recommendation Nos. 2 through 5. Those recommendations are closed upon issuance of this report.

Management comments were included in their entirety in Appendix II.

Scope and Methodology

Scope

The Regional Inspector General/San Salvador conducted this audit, in accordance with generally accepted government auditing standards, to determine if USAID/Bolivia's information system contained general controls to provide assurance that financial information reported was complete, reliable, and secured.

We reviewed the general controls that were in effect at the time of our review over the Unix system that runs the Mission Accounting and Control System (MACS). Our review covered five of the six areas included in the Federal Information System Controls Audit Manual (FISCAM). The five areas covered were security program planning and management, access controls, system software, segregation of duties, and service continuity. We did not cover application software development and change controls because USAID/Bolivia does not develop applications. We also reviewed access settings in MACS to determine if the settings enforced proper segregation of duties between accountants and voucher examiners. Generally, accountants have access to functions that allow them to create projects, agent records, obligations, and commitments. Voucher examiners have access to functions that allow them to prepare and schedule vouchers for payment.

The audit was conducted at USAID/Bolivia from November 26, 2001 through December 13, 2001.

Methodology

We used the Federal Information System Controls Audit Manual to guide our audit testing. In conducting the audit, we interviewed information systems, accounting, and mission management personnel; reviewed security and contingency plans, system files, file permissions, and logs; and observed physical facilities.

We utilized two software tools in conducting the audit. We used "John the Ripper" to decrypt Unix passwords and the "Nessus Security Scanner" to identify system vulnerabilities.

To determine the significance of our findings, we judged that we would issue a positive opinion if we did not note any material weaknesses during our review. Our opinion would be qualified if we noted one or more reportable conditions and negative if we identified one or more material weaknesses. We used the definitions of "material weakness" and "reportable condition" as provided in the General Accounting Office/President's Council on Integrity and Efficiency Financial Audit Manual section 580.33. Those terms are defined as follows:

- **A material weakness** is a reportable condition (see below) in which the design or operation of one or more of the internal control components does

not reduce to a relatively low level the risk that misstatements, whether caused by errors or fraud, losses, or noncompliance in amounts that would be material in relation to the financial statements ... may occur and not be detected within a timely period by employees in the normal course of their assigned duties.

- **Reportable conditions** are matters coming to the auditor's attention that in the auditor's judgement, should be communicated because they represent significant deficiencies in the design or operation of internal control, which could adversely affect the entity's ability to meet the internal control objectives described in the report.

Management Comments

UNITED STATES GOVERNMENT

Memorandum

FMO-02/033

Date	: January 24, 2002
Reply to Attn of	: Tim Cox, Regional Inspector General/ San Salvador
From	: Wayne Nilsestuen, Acting Director USAID/Bolivia
Subject	: Audit of General Controls Over USAID/Bolivia's Mission Accounting and Control System (Report No. 1-511-02- 00X-P)

This memorandum is our response to the draft report on subject audit, and contains responses to the five recommendations included in subject report. We request that you include these comments in your final report.

In addition we have included responses to the Summary Findings which we understand are for management purposes only and will not be included in the final report.

Recommendation No. 1

We recommend that USAID/Bolivia use password management software to enforce password policies.

M/IRM and overseas network administrators are responsible for testing and approving software installed on personal computers and Agency-shared platforms (ADS 550.3.2). USAID/Bolivia requested authorization to use a new product called "Npassword," which enforces complex passwords.

USAID/Bolivia's underlying UNIX operating system (OS) is SUN OS 2.5.1, authorized by M/IRM for MACS and MACSTRAX operations; on October 11, 2001 IRM reviewed our security checklist for the MACS servers. According to M/IRM's UNIX Support Team, this version of the OS does not support complex password programs and other security items. M/IRM is planning to upgrade Solaris V.8 in the second quarter of 2002. In accordance with your recommendation, M/IRM is planning to confirm whether the Solaris OS can handle forced password complexity. M/IRM has promised to keep USAID/Bolivia informed on this as the upgrade comes on line.

In the meantime and as is customary in USAID/Bolivia, at least every three months all users are informed, in writing, to use complex passwords and to follow information security policies. In addition a warning screen is activated upon individual access to the LAN and/or the UNIX environment that illustrates complex password structures.

Recommendation No. 2

We recommend that USAID/Bolivia review log files that detail access attempts and use of sensitive commands.

Previously, a UNIX server script (lapamacs01) automatically compiled and sent a daily back-up log and MACS reconciliation files to USAID/B's EXO/IMS&T staff for evaluation. Per audit recommendations, on December 7, 2001 USAID/Bolivia initiated a new script that additionally sends the log files of access attempts and the use of sensitive commands for evaluation. EXO/IMS&T staff is now reviewing these logs on a daily basis.

Mission requests that the final audit report reflect that this recommendation has been fully implemented and that the finding is closed by the auditors.

Recommendation No. 3

We recommend that access to system commands and programs be restricted to the systems manager.

On November 29, 2001, in accordance with the audit recommendations, the WISP PERSONALITY configuration file was changed for all MACS/MACTRAX users. As a result of these changes access to system commands and programs are restricted to system managers.

Mission requests that the final audit report reflect that this recommendation has been fully implemented and that the finding is closed by the auditors.

Recommendation No. 4

We recommend that USAID/Bolivia include detailed recovery and testing procedures in its contingency plan.

On December 12, 2001 in accordance with the audit recommendations, recovery and testing procedures for UNIX and WINDOWS 2000 environments were added to USAID/Bolivia's Contingency and Risk Assessment Plan. These detailed procedures include the following:

- Introduction
- Preparing for recovery Information UNIX/W2K
- Recovery Flow Charts

  - Generic server rebuilds flow chart UNIX environment
  - Generic Server Rebuild Flow Chart
  - Initial Disaster Recovery Analysis
  - Recovery of Flow Chart
  - Recovery of Flow Chart
  - Recovery of Flow Chart
  - Recovery of 1 Flow Chart
  - Recovery and testing DAT Procedure for UNIX environment
  - Recovering and testing Procedures
  - Recovering and testing Procedures
  - Recovering and testing Procedures
  - Recovering and testing Procedures
  - Schedule of testing procedures for FY 2002/FY 2003

Mission requests that the final audit report reflect that this recommendation has been fully implemented and the finding is closed by the auditors.

Recommendation No. 5

We recommend that the responsibilities for granting functional access in the Mission Accounting and Control System be assigned to someone who does not have accounting duties.

On December 12, 2001, Memorandum FMO 01/389 was issued assigning to Ms. Esmeralda Rodriguez, the Controller's secretary, the primary responsibility of inputting into MACS the functional accesses associated with each MACS User ID.
Ms. Carla Jerez, the Deputy Controller's secretary, was assigned back-up duties to Ms. Rodriguez. Both employees are secretaries and do not have any accounting duties.

Mission requests that the final audit report reflect that this recommendation has been fully implemented and that the finding is closed by the auditors.