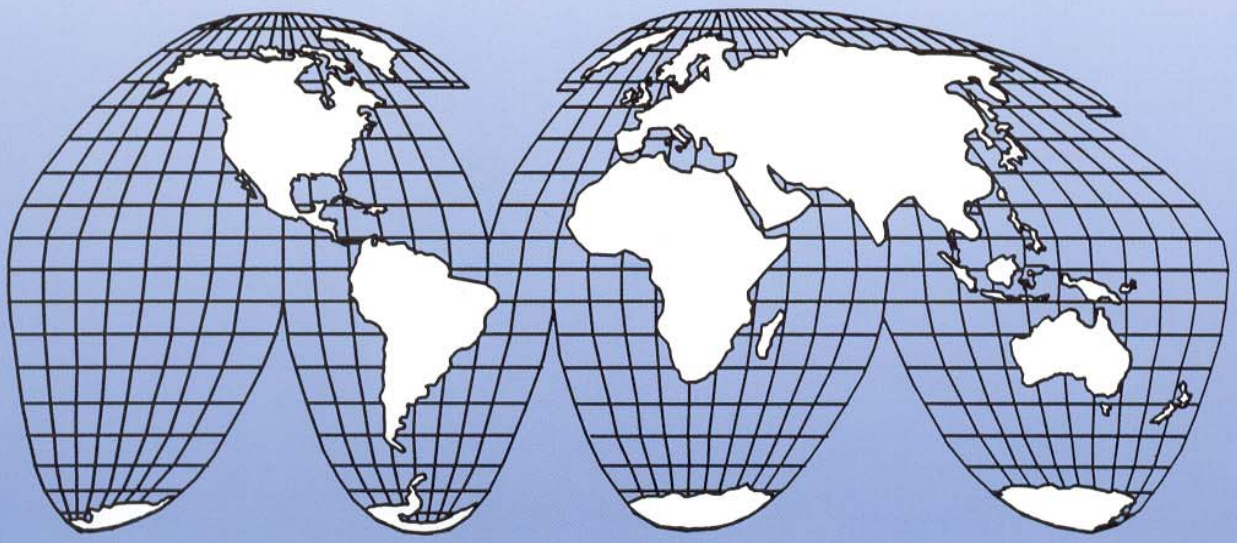
USAID

OFFICE OF INSPECTOR GENERAL

Audit of Follow-up Review of Recommendation No. 1 from Audit Report No. 4-674-02-002-P, Audit of USAID/South Africa's Information Systems General Computer Controls

Audit Report No. 4-674-04-003-P

January 12, 2004



PRETORIA, SOUTH AFRICA

January 12, 2004

MEMORANDUM

FOR: USAID/South Africa Director, Dirk Dijkerman

FROM: Regional Inspector General/Pretoria, Jay Rollins /s/

SUBJECT: Audit of Follow-up Review of Recommendation No. 1 from Audit Report No. 4-674-02-002-P, Audit of USAID/South Africa's Information Systems General Computer Controls (Report No. 4-674-04-003-P)

This memorandum is our report on the subject audit. In finalizing this report, we considered management comments on the draft report and have included those comments, in their entirety, as Appendix II in this report.

This report has two recommendations. In response to the draft report, USAID/South Africa concurred with and included corrective action plans and target completion dates for both recommendations. Therefore, we consider that management decisions have been reached on both recommendations. Please provide the Bureau for Management, Office of Management Planning and Innovation with evidence of final actions in order to close the recommendations.

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

[This page intentionally left blank.]

Table of Contents

[This page intentionally left blank.]

Summary of Results

The Regional Inspector General, Pretoria conducted this audit to determine whether USAID/South Africa took corrective final actions on Recommendation No. 1 of the Office of Inspector General's Audit Report No. 4-674-02-002-P. Recommendation No. 1 included five components for implementing a computer security program at USAID/South Africa (see page 6).

This audit found that USAID/South Africa had taken corrective final actions on three of the five components addressed in Recommendation No. 1. Improvements were made in (1) conducting risk assessments, (2) developing and maintaining an information systems security plan, and (3) implementing effective access controls. However, the Mission's actions did not sufficiently address two components in Recommendation No. 1. The Mission had not adequately prepared and tested an information systems contingency plan nor properly evaluated and monitored the effectiveness of its security program (see pages 7-10).

This report contains two recommendations to help USAID/South Africa improve its computer security program in the two areas mentioned above (see pages 9 and 10).

In response to the draft report, USAID/South Africa concurred with both recommendations contained in the report. The Mission included corrective action plans and target completion dates for both recommendations. Therefore, we consider that management decisions have been reached on both recommendations upon final report issuance (see page 11).

Background

General computer controls are the structure, policies, and procedures that apply to all or a large segment of an entity's information systems and that help ensure their proper operation. The primary objectives of general controls are to safeguard data, protect computer application programs and system software from unauthorized access, and ensure continued computer operations in case of unexpected interruptions. USAID places extensive reliance on information systems to process data. Therefore, it is critical for USAID to maintain adequate internal controls over its financial and management systems. At USAID/South Africa, the Data Management Division (DMD) is responsible for managing, operating and maintaining the Mission's information systems. DMD is responsible for:

- Establishing information system computer processing requirements.
- Processing requests for user access to the system.
- Providing related computer services.
- Monitoring and maintaining the system in compliance with USAID policies and procedures.

On January 15, 2002, the Office of Inspector General (OIG) issued Audit Report No. 4-674-02-002-P. The report addressed OIG concerns regarding USAID/South Africa's ineffective general controls over the computer processing environment. This situation occurred because USAID/South Africa had not implemented a security program that fully met the requirements of the Computer Security Act of 1987, Office of Management and Budget's Circular A-130, or USAID Automated Directives System 545. Therefore, the OIG recommended that USAID/South Africa implement a computer security program that included:

1. Conducting risk assessments.
2. Developing and maintaining an information systems security plan.
3. Implementing effective access controls.
4. Preparing and testing an information systems contingency plan.
5. Evaluating and monitoring the effectiveness of its security program.

Henceforth, for clarity, this audit report will refer to each of the components addressed in Recommendation No. 1 by the numbering scheme provided above.

On March 26, 2003, USAID/South Africa submitted a memorandum to USAID's Office of Management Planning and Innovation (MPI) that requested that MPI close the recommendation made in Audit Report No. 4-674-02-002-P. The memorandum documented actions taken by the Mission and provided information on the implementation of the audit recommendation. Based on the Mission's submission, MPI closed the recommendation on March 28, 2003. The audit in this report covers the period from January 2002 through October 2003.

Audit Objective

This recommendation follow-up audit was conducted in accordance with the U.S. Office of Management and Budget's Circular No. A-50 and Office of Inspector General (OIG) audit policy, which requires the OIG to follow-up on recommendations that have been closed. Specifically, the audit was conducted to answer the following question:

- Has USAID/South Africa taken corrective final actions on Recommendation No. 1 of Audit Report No. 4-674-02-002-P, Audit of USAID/South Africa's Information Systems General Computer Controls?

Appendix I contains a discussion of the audit's scope and methodology.

Audit Findings

Has USAID/South Africa taken corrective final actions on Recommendation No. 1 of Audit Report No. 4-674-02-002-P, Audit of USAID/South Africa's Information Systems General Computer Controls?

USAID/South Africa has taken corrective final actions on three of the five components addressed in Recommendation No. 1. However, the Mission still needs to take further corrective actions on two important components addressed in Recommendation No. 1. These two components relate to developing and testing a contingency plan and to providing a security review.

In response to Recommendation No. 1, the Mission has taken corrective final actions to enhance three components of its general computer controls. These components were related to: conducting risk assessments (component #1), developing and maintaining an information systems security plan (component #2), and implementing effective access controls (component #3). The Mission addressed component #1 by conducting a risk assessment of potential threats and identifying associated countermeasures to mitigate those threats. Component #2 was addressed when the Mission's security plan was approved by Mission management on March 7, 2003, and updated on September 26, 2003. The Mission also implemented effective access controls by having a restricted access-controlled computer server room and by requiring signatures from the Mission's management prior to granting an individual computer system access.[1] Additional access controls included requirements that computer system users need a security clearance and that individuals sign a computer system "rules of individual behavior."[2]

In spite of improvements made, the Mission still needs to take additional corrective actions to further strengthen the Mission's general computer controls. Mission actions did not adequately support preparing and testing an information systems contingency plan (component #4) or evaluating and monitoring the effectiveness of its security program (component #5). Instead of reopening the January 2002 recommendation verbatim, we are rewording a portion of the original recommendation and reissuing it as two new recommendations. These new recommendations will only focus on corrective actions for components #4 and #5, while taking into account the actions that the Mission had already implemented for components #1 through #3.

[1]USAID Computer System Access & Termination Request, AID 545-4 (06/2001).
[2]USAID Unclassified Information Systems Access Request Acknowledgement, AID 545-1 (06/2001).

Mission Contingency Plan Needs To Be Completed and Tested

A complete and tested contingency plan is required by both the U.S. Office of Management and Budget (OMB) under Circular A-130 and by USAID's Automative Directives System (ADS) 545. USAID/South Africa did not have a completed and tested contingency plan. The contingency plan had not been completed because the Mission's staff was involved with other responsibilities that were deemed of higher priority than completing the draft contingency plan. Because the plan was still in draft form, it had not been tested. Until the Mission has a complete and tested contingency plan, the Mission's ability to process, retrieve, and protect information necessary to accomplish its mission in the event of an emergency remains at risk.

Both OMB and USAID have requirements that address the need for developing and testing a contingency plan. OMB's Circular A-130, Appendix III, requires agencies to establish and periodically test systems' capabilities to continue providing service based upon the needs and priorities of system participants. According to ADS 545, the System Manager and designated Information Systems Security Officer (ISSO) must: (1) review, update (if necessary), and test all emergency action plans annually or when significant modifications are made to system hardware, software, or system personnel, and (2) retain copies of the most recent contingency operation, disaster recovery and emergency action plans in the central system file and at the off-site back-up facility. The Directive further states that each member of the system staff and the designated ISSO must receive training in the implementation of emergency procedures and be afforded opportunities to periodically practice the procedures.

Recommendation No. 1, component #4, recommended that USAID/South Africa implement a computer security program that included preparing and testing an information systems contingency plan. When the recommendation was made, the contingency plan was not complete—it lacked several important items. These items included selecting an alternate off-site computing location for emergency situations and selecting members for contingency teams, who would be responsible for responding to emergency situations. At that time, the Mission stated that because it was in the process of transitioning from one operating system to another, it planned to complete and test the contingency plan once the new operating system was installed. However, two years after installing the new operating system, the contingency plan has still not been tested.

The draft contingency plan had not been completed because it had been a lower priority activity for the Mission. Among the higher priorities that faced the staff responsible for the contingency plan was their work related to the Mission's move into its new building in October 2002. Because the contingency plan was not complete, it had not been tested. Until a contingency plan is completed and tested,

the Mission will continue to be exposed to the same vulnerabilities identified in Audit Report No. 4-674-02-002-P. That audit report stated the following:

> *A contingency plan that clearly provides information on supporting resources that will be needed in emergency situations, roles and responsibilities of those who will be involved in recovery activities, and procedures for restoring critical applications and their order in the restoration process would help ensure the Mission's ability to operate if services are interrupted. Without a prepared and tested contingency plan, the Mission may not be able to process, retrieve and protect information maintained electronically or accomplish its mission in emergency situations.*

In conclusion, USAID/South Africa management will need to designate the completion and testing of an information systems contingency plan as a high priority in order to accomplish its mission in emergency situations. Without a complete and tested contingency plan, USAID/South Africa cannot expect its staff to be able to respond positively and efficiently to mitigating emergency situations that may negatively impact the Mission's information systems.

> **Recommendation No. 1: We recommend that USAID/South Africa complete and test its information systems contingency plan**.

Mission Needs to Correct and Complete Its Security Review Questionnaire

OMB's Circular A-130, Appendix III, and USAID's ADS 545 require reviews to assess security controls. ADS 545 specifies the Mission official responsible, in conjunction with other staff members, for performing an annual self-evaluation review of the information systems security program. USAID/South Africa performed a security evaluation of the Mission's information systems, but this effort had inherent problems. In April 2003, the Mission conducted a compliance review of its information systems that contained numerous inaccuracies and non-responses. This occurred because the former Mission staff member who performed the assessment did not use the assistance of Mission's technical staff. The lack of an accurate and complete computer security review has resulted in the Mission having a diagnostic tool that it cannot rely upon to identify and mitigate computer security risks.

OMB's Circular A-130, Appendix III, states that agencies should review the security controls in each system when significant modifications are made to the system, or at least every three years. USAID's ADS 545 goes further by making the Information Systems Security Officer (ISSO) responsible for conducting annual self-evaluation reviews of the information systems security program managed by the ISSO. The Unclassified Information System Compliance Review

questionnaire (AID 545-3 [6/2001]) states that the ISSO "in conjunction with the Program Manager, System Manager/IT Specialist and other appropriate security personnel, must use this questionnaire." The questionnaire must be used for "conducting an annual review of the security posture of each system operating in support of their mission or program." Further, AID 545-3 states that the questionnaire was developed for use as a guideline, and that the ISSO must use the questionnaire for "assessing compliance with Federal and USAID information systems security policies, procedures and regulations governing electronic data processing and storage." All noted deficiencies in the review are required to be addressed in a corrective action plan.

Recommendation No. 1, component #5, recommended that USAID/South Africa implement a computer security program that included evaluating and monitoring the effectiveness of its security program. In response to this recommendation, on April 23, 2003, a Mission official performed a security review using the AID 545-3 questionnaire. However, of the questionnaire's 43 questions, 7 had incorrect answers and 13 were not answered. An example of one of the questions incorrectly answered was "Have the contingency operation plans been successfully practiced or implemented within the last year?" The incorrect response was "yes". An example of one of the questions not answered was "Are up-to-date contingency operation plans in place?"

The problems with the April 2003 security review were attributed to a lack of knowledge by the former ISSO who completed the review. According to Mission staff, the former ISSO official who completed the questionnaire did so without the assistance of the Mission's technical staff. In addition, the unanswered questions may have reflected unfamiliarity with the Mission's information system.

The lack of an accurate and complete computer security review has resulted in the Mission having a diagnostic tool that it cannot rely upon to identify and mitigate computer security risks. In conclusion, based on the significant problems identified with the current security review, we believe it would be prudent for the Mission to correct and complete its 2003 security review. Therefore, we are making the following recommendation.

Recommendation No. 2: We recommend that USAID/South Africa correct and complete its April 2003 security review questionnaire to better evaluate and monitor the effectiveness of its security program.

Management Comments and Our Evaluation

In response to our draft report, USAID/South Africa management concurred with Recommendation Nos. 1 and 2. The Mission also provided corrective action plans and target completion dates for both recommendations. Therefore, we consider that management decisions have been reached for both recommendations upon final report issuance.

[This page intentionally left blank.]

Scope and Methodology

Scope

The Regional Inspector General/Pretoria conducted this audit in accordance with generally accepted government auditing standards. The audit, covering the period from January 2002 through October 2003, reviewed the corrective final actions taken by the Mission on Recommendation No. 1 from our January 2002 audit report on USAID/South Africa's general computer controls. In planning and performing the audit, we tested and assessed significant management controls related to the Mission's information systems. In this effort, we tested the process used by the Mission to ensure that its employees and visitors obtain the appropriate authorization in order to access to the Mission's information systems. Further, we also assessed the management controls used to protect the Mission's information systems from unauthorized users and prohibited uses. The types of evidence examined during the audit included—but were not limited to—the Mission's Security Plan and draft Contingency Plan, relevant documents concerning the Mission's efforts to improve computer controls, and testimony from USAID/South Africa staff. The audit was conducted at USAID/South Africa in Pretoria, South Africa, from September 25 to October 21, 2003.

Methodology

The purpose of this audit was to review the Mission's corrective final actions on Recommendation No. 1. Specifically, the audit was designed to answer the question, "Has USAID/South Africa taken corrective final actions on Recommendation No. 1 of Audit Report No. 4-674-02-002-P, Audit of USAID/South Africa's Information Systems General Computer Controls?" To answer the audit's objective, we reviewed Mission documents and interviewed Mission officials. Some of these documents included the Mission's (1) memorandum recommending the closure of Recommendation No. 1 to USAID's Office of Management Planning and Innovation, (2) April 2003 security review, (3) draft contingency plan, (4) security plan, (5) completed computer system access forms, and (6) computer security training list of participants.

We also relied upon Audit Report No. 4-674-02-002-P (issued by RIG/Pretoria on January 15, 2002), on which this review was based, in order to (1) identify and review the criteria that had been used and (2) gain an understanding of the reported findings. We reviewed each of the five components that comprise Recommendation No. 1 and the associated critical findings identified in the prior audit report. For each finding, we determined if the problem areas had been addressed. These determinations were based on professional judgment and served as the basis for deciding whether to concur that reported final actions effectively addressed components in Recommendation No. 1. In the two instances where the Mission's actions did not effectively address the specific components in Recommendation No. 1, we decided to reopen those particular components.

The nature of this audit did not lend itself to materiality thresholds; thus none were developed.

Management Comments

January 2, 2004

MEMORANDUM

TO: Jay Rollins, RIG/Pretoria

FROM: Dirk Dijkerman, Mission Director /s/

SUBJECT: Management Comments to Follow-up Audit to Audit Report No. 4-674-02-002-P

Executive Office/Data Management Division staff reviewed the recommendations of the subject audit report and I concur with their proposed management comments reproduced below:

Recommendation No. 1: We recommend that USAID/South Africa complete and test its information systems contingency plan.

USAID/South Africa intends to complete its information systems contingency plan in January 2004 and test the plan no later than February 29, 2004.

Recommendation No. 2: We recommend that USAID/South Africa correct and complete its April 2003 security review questionnaire to better evaluate and monitor the effectiveness of its security program.

USAID/South Africa intends to have a qualified official re-administer the Unclassified Information System Compliance Review questionnaire prescribed by ADS 545-3 no later than March 31, 2004 and annually thereafter (or more frequently should significant system modifications be carried out).

cc: ESchaeffer, RFMO
LNortje, EXO/DMD

Cleared: BSchaeffer, EXO /s/

KFickenscher, A/DD /s/