

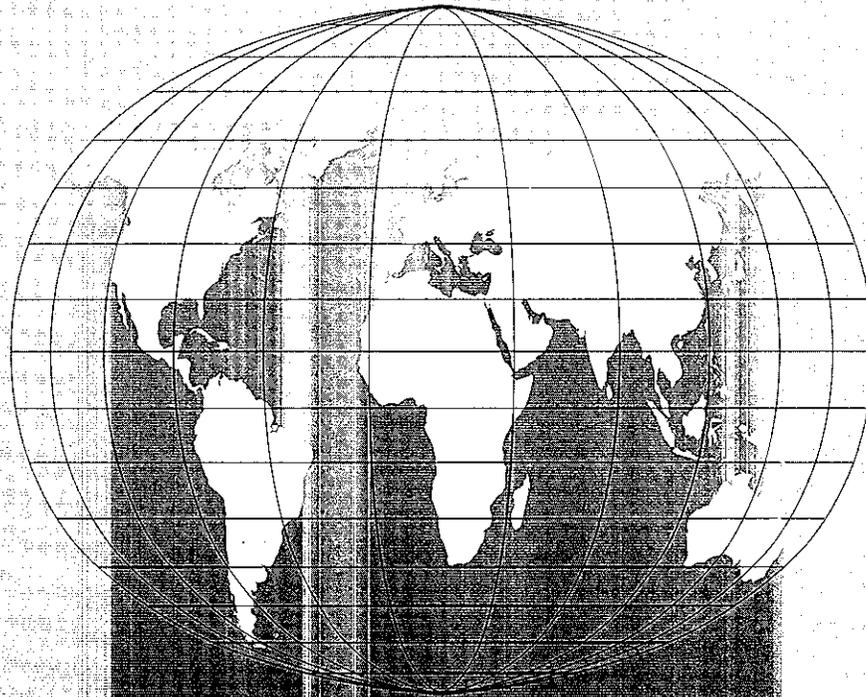
PD-ABU-729

113130

Report of Audit

Audit of USAID/South Africa's Information Systems General Computer Controls

Report No. 4-674-02-002-P
January 15, 2002



PRETORIA SOUTH AFRICA
OFFICE OF INSPECTOR GENERAL
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT



U.S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

RIG/Pretoria

January 15, 2002

MEMORANDUM

FOR: Director, USAID/South Africa, *Dirk W. Dijkerman*
FROM: Regional Inspector General/Pretoria, *Joseph Farinella*
SUBJECT: Audit of USAID/South Africa's Information Systems General
Computer Controls, Audit Report No. 4-674-02-002-P

This memorandum is our report on the subject audit. We received your comments to our draft report and included those comments as Appendix II to this report.

This report contains one recommendation to implement a computer security program. Based on your agreement to implement such a program, a management decision has been reached on Recommendation No.1. Please advise the Bureau for Management, Office of Management Planning and Innovation, Management and Innovation Control Division (M/MPI/MIC) when final action is complete.

Thank you for 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	
Are USAID/South Africa's general controls over the computer- processing environment effective?	4
Conduct Risk Assessments	5
Develop a Security Plan	6
Implement Effective Access Controls	8
Prepare and Test a Contingency Plan	9
Evaluate and Monitor its Security Program	10
Management Comments and Our Evaluation	12
Appendix I - Scope and Methodology	13
Appendix II – Management Comments	15

Summary of Results

Our audit of USAID/South Africa's Information Systems General Computer Controls focused on whether the general controls over the computer-processing environment were effective.

We found that USAID/South Africa's general controls over the computer-processing environment were not effective. This 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 (OMB) Circular A-130, or USAID Automated Directive Systems (ADS) (page 4).

To strengthen controls, the Mission should implement a security program that includes conducting risk assessments (page 5); developing a security plan that complies with OMB Circular A-130, Appendix III (page 6); implementing effective access controls (page 8); preparing and testing an adequate contingency plan (page 9); and evaluating and monitoring the effectiveness of its security program (page 10).

These areas are discussed in more detail in the *Audit Findings* section of this report.

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 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. The effectiveness of general controls is a significant factor in ensuring the effectiveness of application controls. Application controls are controls over the input, processing, and output of data associated with individual computerized applications. Without effective general controls, application controls may be rendered ineffective by circumvention or modification.

USAID places extensive reliance on information systems to process data. It is, therefore, critical for USAID to maintain adequate internal controls over its financial and management systems. In 1998 and 1999, the Office of Inspector General (OIG) found that USAID did not have effective general controls over financial systems that operate on the mainframe, client-server and UNIX computer environments. For example, USAID had not established: (1) an entity-wide security program, (2) access controls, (3) application software development and change processes, and (4) segregation of computer system duties over the mainframe computer systems. Consequently, the OIG recommended corrective actions to address these deficiencies. In response to the OIG's recommendations, USAID management had taken some actions to improve its general controls over its financial management systems.

USAID/South Africa's Data Management Division (DMD) is responsible for managing, operating and maintaining the Mission's information systems. Specifically, DMD is responsible for: (1) establishing information system computer processing requirements; (2) processing requests for user access to the system; (3) providing related computer services and (4) monitoring and maintaining the system in compliance with USAID policies and procedures.

Audit Objective

As part of a USAID-wide review, RIG/Pretoria performed this audit to answer the following question:

Are USAID/South Africa's general controls over the computer-processing environment effective?

Appendix I provides a complete discussion of the scope and methodology for this audit.

Audit Findings

Are USAID/South Africa's general controls over the computer-processing environment effective?

USAID/South Africa's general controls over the computer-processing environment were not effective. This occurred because USAID/South Africa had not implemented a security program that fully met the requirements of The Computer Security Act of 1987¹, OMB Circular A-130 Appendix III² or USAID's Automated Directive System (ADS)³. Without implementing an effective security program, risks may not be clearly understood, controls may not be effective and large amounts might be spent to protect against low-risk threats. Not implementing a complete security program precludes effective general controls.

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, states that agencies shall implement and maintain a program to assure that adequate security is provided for all agency

¹ According to the Computer Security Act of 1987, Federal agencies with computer systems that process sensitive information are required to identify and develop security plans for these systems and to provide security training to persons managing, using, and operating these systems.

² OMB Circular A-130, Appendix III, establishes a minimum set of controls to be included in Federal automated information systems security programs. These controls include assigning security responsibilities, preparing security plans, conducting security reviews, accrediting systems and providing security incident reporting capabilities.

³ ADS Chapter 545 titled Information Systems Security documents the Agency's security policies and procedures for its information systems security program and lists specific headquarters and mission responsibilities.

information collected, processed, transmitted, stored, or disseminated in general support systems.

A security program provides the foundation for effective general computer controls—entity-wide security program planning, access controls, application software development and change processes, segregation of computer system duties, system software and service continuity—in a computer environment.

Major elements (under the general control categories of entity-wide security program planning, access controls and service continuity) of a security program that the Mission had not fully implemented were:

- conducting risk assessments of its computer operations;
- developing a security plan that complied with OMB Circular A-130, Appendix III;
- implementing effective access controls;
- preparing and testing an adequate contingency plan; and
- evaluating and monitoring the effectiveness of its security program.

These areas are discussed in detail below.

Conduct Risk Assessments

OMB Circular A-130, Appendix III, states, “While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management [such as] the value of the system, threats, vulnerabilities and the effectiveness of current or proposed safeguards.”

The Mission had not conducted a risk assessment to identify the threats and vulnerabilities to its systems as required. This occurred because the Mission was in the process of transitioning from one operating system to another operating system. The Mission stated that it planned to conduct a risk assessment once the new operating system was implemented.

In June 2001, the Mission requested the Bureau for Management’s Office of Information Resources Management (M/IRM) Washington to review the Mission’s information technology program. M/IRM’s review specifically focused on: (1) the staffing and organization structure of the data management division (DMD), (2) communication between DMD, management and the end user and (3) a review of the existing network to identify and correct deficiencies to ensure readiness to support new initiatives. To support the review, the Mission completed a checklist that included a

component on information security. However, this checklist only covered general information technology issues. It was not an in-depth review of the possible threats and vulnerabilities to its system. The Mission indicated in the checklist that a risk assessment had been recently performed of its systems. DMD could not provide this assessment and the staff stated that to its knowledge a risk assessment had not been performed of its systems. As a result of not conducting risk assessments, the Mission may not be aware of weaknesses that may exist on its systems.

A risk assessment is a crucial element of the security planning process and determines the control measures needed to protect the systems. To assist the Mission in identifying potential threats and vulnerabilities to its systems and any additional security measures that may be needed, a thorough information technology risk assessment should be periodically performed and documented.

Develop a Security Plan

According to OMB Circular A-130, Appendix III, to comply with the Computer Security Act, security plans must be developed for all Federal computer systems that contain sensitive information.

The Circular provides specific controls, as well as detailed information on the controls, that should be included in a security plan. They are: (1) rules of the system, (2) training, (3) personnel controls, (4) incident response capability, (5) continuity of support, (6) technical security and (7) system interconnection.

The Mission did not have a fully developed or comprehensive security plan that incorporated the security controls prescribed by the Circular. This occurred because the Mission did not follow the security plan template, which is available on USAID's Information Systems Security Program website. The template was designed by Bureau for Management's Office of Information Resources Management to meet the requirements of OMB Circular A-130, Appendix III. Instead, the Mission presented various documents, which collectively contained some of the required topics of a security plan. Personnel, technical security and system interconnection controls were complete and fully developed. However, as discussed below, rules of the system, training, incident response capability and continuity of support were not complete or fully developed. As a result, the users of the systems may not be fully aware of the rules or policies and procedures associated with the systems, which could lead to the systems being compromised.

Rules of the System- According to OMB Circular A-130, Appendix III, rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. Specifically, the rules should cover such matters as

work at home, dial-in access, connection to the Internet, use of government equipment, the assignment and limitation of system privileges and individual accountability. In addition, they should state the consequences of behavior not consistent with the rules. Mission documents covered these areas except for work at home, dial-in access and the consequences of non-compliance. Work at home and dial-in access are areas of high vulnerability. These areas should be complete and fully developed to provide adequate security of the Mission's system and all users should be aware of the consequences of non-compliance. However, we noted that the Mission does have technology controls in place such as an internal firewall, user identifications and passwords which helps protect against intrusion or unauthorized access.

Training- OMB Circular A-130, Appendix III, states that the Computer Security Act requires federal agencies to provide for mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use or operations of a federal computer system. The Circular further states that all individuals should be appropriately trained in their security responsibilities—before allowing them access to the system—and periodically provided refresher training to assure that they continue to understand and abide by the applicable rules.

The Mission provided such training on an ad-hoc basis and it was not fully documented or applied consistently. Specifically, the Mission did not always distribute documents describing security policies, procedures and individual responsibilities or provide a security orientation, training or periodic refresher programs to new and current employees. For example, at the time of our audit three of eight recently-hired employees had received some form of written documentation on the system's security policies, rules and expected behavior and two others had received impromptu training on computer security awareness. The Mission stated that a more uniformly applied platform of computer awareness training for all computer users was being planned.

Incident Response Capability- According to OMB Circular A-130, Appendix III, agencies should establish a formal incident response capability. Such capability will ensure agencies will be able to respond in a manner that protects both their own information and the information of others when faced with a security incident. ADS 545 also states, in part, that the system administrator should log all anomalies that are a result of a technical glitch, not just the result of wrongful actions by unauthorized people. It further requires the system administrator to maintain an event log, noting date and time, summarizing the anomaly and describing his or her own activities and those of the possible intruder.

DMD investigates and responds to reported incidents but there is no formal incident response capability that allows users to make requests and report

problems. Specifically, there is no formal mechanism or central point of contact such as a central email box for users to make requests or report computer-related problems. When users make requests or report problems, it is done by sending an email or telephoning one of the DMD's staff members. The problem or request is addressed but this method does not provide a historical record of problems because DMD does not log nor track all problems. Several years ago, the Mission established logbooks to record anomalies. Our review of the logbooks indicated that with the exception of one entry made on June 6, 2001, no entries had been made since 1995.

Establishing a formal incident response capability and maintaining and periodically reviewing logs would help ensure that problems are addressed in a timely manner and that corrective actions are taken. It would also provide a historical record to identify remedies for recurring problems and training needs for users.

Continuity of Support- This area is discussed under the section, "Prepare and Test a Contingency Plan."

The purpose of a security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. Without a fully developed and comprehensive security plan, the Mission systems are at a higher risk for misuse, modification or destruction.

Implement Effective Access Controls

ADS 545 requires that all individual USAID employees or contractor-users complete a USAID Computer System Access and Termination Request form and a USAID Unclassified Information Systems Access Request form before direct access is granted to any USAID information system. A U.S. direct hire employee must approve these forms.

Access requests were not documented on standard forms, maintained in files and/or approved by senior managers. This occurred because the Mission used email notifications from the various offices to grant access to its systems. During our fieldwork, the Mission implemented one part of the requirement by having all users complete the USAID Computer System Access and Termination Request form.

ADS 545 further states that Managers and Division Chiefs must provide the designated Information Systems Security Officer (ISSO) with written notification of a user's system termination no later than one working day after the user no longer requires system access. The ISSO must forward the written

notice to the Information Technology (IT) Specialist for action. The IT Specialist must retain user system termination notifications in the central system file for at least six months after the date the user is removed from the system.

For U.S. direct hires and personal service contractors, the DMD completes a standard checklist signifying that the person's access rights to the system have been removed. The documentation was maintained in the files. However, a similar procedure is not followed for Foreign Service Nationals, temporary duty employees and contractors. The Mission did not maintain documentation on terminating these users. Although our testing did not reveal any unauthorized access to the Mission's system or user accounts still active for recently terminated or departed employees, it is important that the terminations are documented and maintained to ensure that users be removed and the security of the system is safeguarded.

Access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss or impairment. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

Prepare and Test a Contingency Plan

OMB Circular A-130, Appendix III, requires agencies to establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of system participants.

According to ADS 545, the System Manager and designated 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 backup facility. It 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.

The Mission's contingency plan was developed in June 2001. However, the plan was not complete. The plan did not contain procedures to protect actual data on a system-by-system or connection-by-connection basis which is covered in a Connection Security Plan component of a contingency plan. This component had yet to be developed by the Mission. Also, the plan did not identify or provide information on supporting resources that would be needed, roles and responsibilities of those who would be involved in recovery activities, and procedures for restoring critical applications and their order in

the restoration process. At the time of our audit, the plan had not been tested and copies were not maintained at the off-site storage location. Also, the DMD had not been trained in its responsibilities during emergency situations. This occurred because the Mission was in the process of transitioning from one operating system to another operating system. The Mission stated that it planned to prepare and test the contingency plan once the new operating system was implemented.

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.

Evaluate and Monitor its Security Program

OMB Circular A-130, Appendix III, states that agencies should review the security controls in each system when significant modifications are made to the system, but at least every three years. ADS 545 goes even further by stating that the ISSO is responsible for conducting annual self-evaluation reviews of the information systems security program managed by the ISSO.

The Mission had not reviewed its computer security controls either at three-year intervals or on an annual basis. Specifically, the Mission had not developed procedures to determine if the controls were operating as intended or evaluated the effectiveness of the program in communicating policies, raising awareness levels and reducing incidents. This occurred because the Mission did not have a formal program or procedure to periodically examine the system for vulnerabilities that could result from improper use of controls or mismanagement. Consequently, general control weaknesses such as those identified in this report exist and expose information resources to unauthorized use, modification, and destruction.

In conclusion, a security program provides the foundation on which effective general computer security practices can be implemented. Establishing a framework for planning and managing activities to assess risk, developing and implementing security procedures, and monitoring the effectiveness of the procedures helps ensure that sensitive data and resources will be protected. Without a comprehensive security program, risks may not be clearly understood, controls may not be effective and large amounts might be spent to protect against low-risk threats.

Therefore, we are making the following recommendation:

Recommendation No.1: We recommend that USAID/South Africa implement a computer security program that includes (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; and (5) evaluating and monitoring the effectiveness of its security program.

**Management
Comments and
Our Evaluation**

USAID/South Africa officials concurred with the recommendation to implement a computer security program. In response to the recommendation, USAID/South Africa stated that the Data Management Division has already begun developing monitoring, evaluation and testing procedures for implementation. Also, IT [information technology] operating system policies to safeguard the integrity and security of the Mission's systems will be implemented.

Based on USAID/South Africa's response, Recommendation No. 1 is classified as having reached a management decision.

**Scope and
Methodology**

Scope

Our audit was performed in accordance with generally accepted government auditing standards and ascertained whether USAID/South Africa's general controls over the computer-processing environment were effective. This audit was part of the Government Management Reform Act audit that was conducted USAID-wide.

Criteria used to evaluate the results were OMB Circular A-130, Appendix III, applicable sections of the Automated Directive Systems (ADS), and laws and regulations such as the Computer Security Act of 1987. To assist in evaluating the general controls, we used GAO's Federal Information Systems Control Audit Manual (FISCAM).

The audit was conducted at USAID/South Africa in Pretoria, South Africa from August 6 to 29, 2001.

Methodology

The audit objective was to determine whether USAID/South Africa's general controls over the computer-processing environment were effective.

To answer the audit objective, we identified and reviewed the Mission's information system's general control policies and procedures. We documented the extent to which the Mission implemented the controls and their effectiveness. We also held discussions with pertinent staff members of the Controller's Office, which manages the Data Management Division, and the Executive Office.

To assist us in identifying and evaluating the general controls, we used the GAO's FISCAM. GAO divided the general controls into six categories.

For the six categories, we tested the critical elements, identified by GAO, that are essential for establishing adequate controls. For each critical element, we made a determination as to the effectiveness of the Mission's related controls. If the controls for one or more of each category's critical elements were ineffective, then the controls for the entire category were deemed to be ineffective. Professional judgment was used in making such determinations.

The definitions for each category follow:

Entity-Wide Security Program Planning

Provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

Access Controls

Limit or detect access to computer resources (data, programs, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss and disclosure.

Application Software Development and Change Controls

Prevent unauthorized programs or modifications to an existing program from being implemented.

Segregation of Duties

Ensure policies, procedures, and organizational structure are established so that one individual cannot control key aspects of computer related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

System Software

Limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

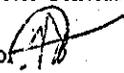
Service Continuity Controls

Ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

**Management
Comments****UNITED STATES GOVERNMENT
MEMORANDUM**

DATE : January 8, 2002

TO : Joseph Farinella, Regional Inspector General/Pretoria

FROM : Dirk Dijkerman, Mission Director 

SUBJECT : Audit of USAID South Africa's Information Systems General Computer Controls

The purpose of this memorandum is to advise that we have received the draft audit report, which summarizes the results of the audit of the Mission's computer system controls. We concur with the recommendation that USAID South Africa implement a computer security program that includes conducting a risk assessment and implementation of comprehensive IT system security and contingency plans.

In response to this report, the Data Management Division of the Executive Office has already begun developing monitoring, evaluation and testing procedures for implementation. Additionally, IT operating system policies that safeguard the integrity and security of the Mission's IT systems will also be implemented. Once the plans are finalized and tested the information will be sent to M/MPI for final action and closure of the audit recommendation.

We would like to take this opportunity to commend the professional and cooperative manner in which your staff conducted the audit of our IT systems.