

PD-ABW-073

113816

# USAID

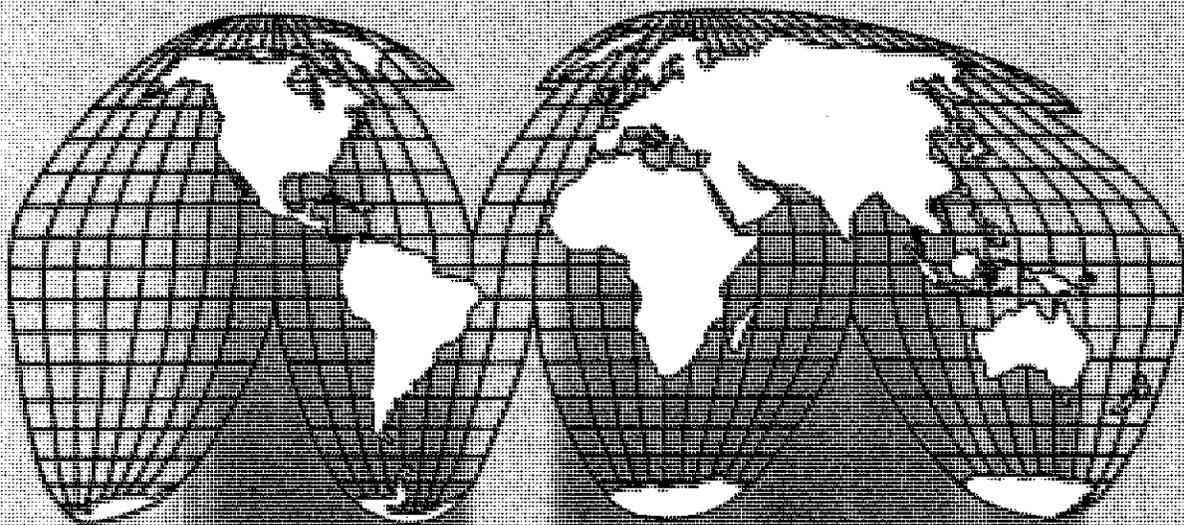
## OFFICE OF INSPECTOR GENERAL

---

### Audit of USAID/Egypt's Information Systems' General Computer Controls

Audit Report No. 6-263-02-003-P

February 3, 2002



U.S. Agency for International Development

Washington, D.C.



U.S. AGENCY FOR  
INTERNATIONAL  
DEVELOPMENT

*RIG/Cairo*

February 3, 2002

## MEMORANDUM

**FOR:** Director, USAID/Egypt, Willard J. Pearson Jr.

**FROM:** RIG/Cairo, <sup>*D. Burris*</sup> Darryl T. Burris

**SUBJECT:** Audit of USAID/Egypt's Information Systems' General Computer Controls (Report No. 6-263-02-003-P)

This is our final report on the subject audit. We reviewed your comments to our draft report and included them as Appendix II to this report.

The report contains one recommendation for USAID/Egypt to develop a computer security program. Based on your comments to our draft report, we consider that a management decision has been made on Recommendation No. 1. Please notify the Bureau for Management's Office of Management Planning and Innovation when final action is complete.

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

---

---

**Table of  
Contents**

	<u>Page</u>
Summary of Results	3
Background	3
Audit Objective:	4
Were USAID/Egypt's General Controls Over its Computer- Processing Environment Effective?	
Audit Finding:	4
USAID/Egypt Needed to Implement an Effective Information Security Program	4
Management Comments and Our Evaluation	8
Appendix I - Scope and Methodology	9
Appendix II - Management Comments	10
Appendix III - GAO's Categorization of General Controls	14
Appendix IV - Detailed Listing of Audit Findings	15

---

## Summary of Results

The Regional Inspector General/Cairo audited the effectiveness of USAID/Egypt's general controls over its computer-processing environment. USAID/Egypt's general computer controls were not effective, but Mission officials said that they were unaware of any adverse effects (e.g., data loss or computer system security breaches) resulting from the ineffective controls. Nonetheless, sensitive data, assets, and computer resources were vulnerable to unauthorized access, modification, loss, or destruction. (See page 4.)

This report focuses on USAID/Egypt's information security program as the primary cause for the weaknesses in the Mission's general controls. (See page 4.) To strengthen these controls, we recommended that the Mission develop a computer security program that includes developing and maintaining an information systems security plan; implementing effective access controls; preparing and testing an information systems contingency plan; and monitoring and evaluating the effectiveness of the overall security program. (See page 7.)

---

## 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.

USAID places extensive reliance on information systems to process financial statement data. It is, therefore, critical for USAID to maintain adequate internal controls over the systems that support the financial statements. In 1998 and 1999, the Office of Inspector General (OIG) reported that USAID did not have effective general controls over financial systems that operated 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 improved its general controls over its financial management systems. Since then, however, USAID implemented the core financial management module to the new financial management system in Washington, D.C. that required changes to the supporting computer environments. Also, security improvements were made to accounting systems at USAID missions. To minimize risks to USAID's sensitive and critical financial systems, the general controls over the new and upgraded computer systems were being evaluated. Our audit at USAID/Egypt was a part of this evaluation.

---

---

## Audit Objective

This audit represented one of an Agencywide series of audits carried out by USAID's Office of Inspector General. This audit was performed by the Office of Inspector General's regional office in Cairo, Egypt and answered the following audit objective:

Were USAID/Egypt's general controls over its computer-processing environment effective?

Appendix I presents the audit scope and methodology.

---

## Audit Findings

**Were USAID/Egypt's general controls over its computer-processing environment effective?**

USAID/Egypt's general controls over its computer-processing environment were not effective. Although the controls were not effective, Mission officials said that they were unaware of any adverse effects (e.g., data loss or computer system security breaches) resulting from the ineffective controls. Nonetheless, sensitive data, assets, and computer resources were vulnerable to unauthorized access, modification, loss, or destruction.

This report focuses on USAID/Egypt's information security program as the primary cause for the weaknesses in the Mission's general controls. That is, although USAID/Egypt had implemented several components of an information security program, including: (1) assigning user identifications and passwords; (2) requiring backup copies of Mission Accounting and Control System data to be stored off-site; and (3) using encrypted password files and suppressed passwords; as discussed in the following section, the Mission's program was not effective and did not meet USAID requirements.

### **USAID/Egypt Needed to Implement an Effective Information Security Program**

The Computer Security Act of 1987<sup>1</sup>, the Office of Management and Budget's Circular A-130<sup>2</sup>, and USAID's Automated Directives System<sup>3</sup> provide policies and procedures for establishing information systems security programs. However, due

---

<sup>1</sup> 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 provide security training to persons managing, using, and operating these systems.

<sup>2</sup> The Office of Management and Budget's (OMB) Circular A-130 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, and providing security incident response capabilities.

<sup>3</sup> Chapters 545 and 552 titled Automated Information Systems Security and Classified Information Systems Security, respectively, document USAID's security policies and procedures for information systems security and list specific headquarters and mission responsibilities.

---

to three office moves in the last three years and a high turnover in the Mission's systems manager position, USAID/Egypt had not implemented an effective information security program. Consequently, several weaknesses in the Mission's general controls existed, and sensitive data, assets, and computer resources were vulnerable to unauthorized access, modification, loss, or destruction.

An organization-wide computer security program provides the foundation on which effective computer security practices can be implemented. By establishing a framework for planning and managing activities to assess risks, develop and implement security procedures, and monitor the effectiveness of the procedures, a security program helps ensure that sensitive data and resources will be protected in a cost-effective manner. Without a security program, risks may not be clearly understood, controls may not be effective, and large dollar amounts might be spent to protect against low-risk threats.

USAID/Egypt had not implemented an effective computer security program due, in part, to three office moves in the last three years and a high turnover in the Mission's systems manager position. The three office moves diverted personnel resources<sup>4</sup> from resolving system security issues to getting systems up and running in new office buildings. In regards to the Mission's systems manager position, the acting systems manager during our audit was the Mission's third systems manager in the last 12 months.

The major requirements and practices that USAID/Egypt had not fully implemented are as follows (a detailed listing of audit findings is included in Appendix IV):

- developing an information systems security plan;
- implementing effective access controls;
- preparing and testing an adequate contingency plan; and
- evaluating and monitoring the effectiveness of its security program.

The following sections discuss these four issues.

**Developing an Information Systems Security Plan** – Under the Computer Security Act, OMB Circular A-130, and USAID's Automative Directives System, Chapter 545.3.1.3, USAID/Egypt was required to prepare and implement security plans for protecting systems that contain sensitive data. The security plans should document the security requirements of systems and describe how USAID will meet the requirements.

---

<sup>4</sup>USAID/Egypt's Data Management System division, which is part of the Management Office, is responsible for operating the Mission's information resources. For example, it is responsible for: (1) establishing information system computer processing requirements and implementing an effective security program; (2) processing all requests for computer access to the system; and (3) providing system computer services.

---

USAID/Egypt had developed a security plan, but it was not signed or dated. The plan was also not current and did not cover all of the topics prescribed by OMB Circular A-130. For example, the plan did not identify who owns the Mission's computer resources or establish a security management structure.

**Implementing Effective Access Controls** – As required by Automated Directives System Chapter 545.3.2.4, a USAID Computer System Access and Termination Request form must be completed for each staff member requiring interactive system access.

Contrary to this requirement, USAID/Egypt granted system access to new users based on e-mail requests. USAID/Egypt also did not effectively review users of its systems to those authorized to use them. As a result, 6 of 14 employees, who had left the Mission between December 2000 and June 2001, still had access to the Mission's computer systems although they were no longer employed at the Mission.

USAID/Egypt used a departure checklist that must be completed by each departing employee. This checklist included the Data Management System Office, which was then supposed to remove the departing employee's access from the Mission's computer system. However, Data Management System personnel signed off on the checklist without always deleting the employee from the computer system.

In addition, contrary to controls outlined in the Federal Information System Controls Audit Manual, access to system software was not limited to employees identified as system software specialists. Further, responsibilities for monitoring the use of system utilities (i.e., system diagnostic and support tools) were not defined or assigned. Consequently, although USAID/Egypt's computer system had a built in function that allowed for the logging of all events occurring in the system, Mission officials said these logs had never been reviewed. A lack of management reviews and monitoring of the logs could result in inappropriate or unusual activities going undetected.

**Preparing and Testing an Adequate Contingency Plan** – To ensure that critical operations can continue in emergencies, Automated Directives System Chapter 545.3.2.5 requires a plan to cope with potential loss of operational capability.

USAID/Egypt developed a contingency plan, but the plan was not dated or signed. The plan also did not identify the Mission's back up facility, responsibilities assigned to personnel, or detailed instructions for data recovery. Further, Mission officials said that the contingency plan, which was supposed to be tested annually, had never been tested. Without an adequate contingency plan and a test of that plan, USAID/Egypt faced high risks that its computer operations could be seriously impaired should a major service disruption or disaster occur.

---

**Evaluating and Monitoring Its Security Program** – As required by Automated Directives System Chapter 545.2, USAID/Egypt's Management Office, which is headed by an Executive Officer, was responsible for implementing USAID's Information System Security Program at USAID/Egypt.

The Executive Officer, however, generally relied on the Mission's Systems Manager to establish and maintain a computer security program and, thus, had not evaluated or systematically monitored the Mission's information security program. Consequently, the Mission had not yet adequately addressed 3 of 20 vulnerabilities that had been identified in an August 1999 information system risk assessment. The three vulnerabilities were as follows:

- Lack of an ongoing system security training program that can be included in an overall Mission Security Program Plan;
- Users not required to sign a Systems Access Agreement form prior to gaining access to the network; and
- Lack of an authorized access list with emergency contacts posted on the entrance to the computer room.

The Management Office had also not (1) implemented procedures<sup>5</sup> to determine if security controls were operating as intended or (2) evaluated the effectiveness of the program in communicating policies, raising awareness levels, and reducing incidents. For instance, USAID/Egypt had not examined the system for vulnerabilities that could result from improper use of controls or mismanagement. Subsequently, general control weaknesses, such as those identified in this report, existed and exposed information resources to unauthorized use, modification, and destruction.

\* \* \* \* \*

Effective general computer controls require attention to maintain the integrity, availability, and performance of sensitive systems in a complex computer environment. While USAID/Egypt had taken some measures, its general controls over the computer-processing environment were not effective. To adequately protect sensitive data and systems from unauthorized access, disclosure, and loss, USAID/Egypt needed to implement an effective computer security program. Therefore, we recommended the following:

**Recommendation No. 1: We recommend that USAID/Egypt develop a computer security program that includes:**

- 1.1 developing and maintaining an information systems security plan;**

---

<sup>5</sup> We were provided a draft Mission Order on information system security.

- 
- 1.2 **implementing access controls in compliance with Automated Directives System Chapter 545.3.2;**
  - 1.3 **preparing and testing an information systems contingency plan; and**
  - 1.4 **monitoring and evaluating the effectiveness of its security program.**

---

**Management  
Comments and  
Our Evaluation**

In response to our draft report, USAID/Egypt said that it was committed to implement an Information Systems Security Program and agreed on the necessity of implementing effective controls to secure its information. The Mission also said that it would implement the report's recommendation.

In response to Recommendation No. 1.1, the Mission said that it had started developing an updated Information System Security Plan and that the updated plan would be completed by December 1, 2002.

In regards to Recommendation No. 1.2, the Mission explained that it had already taken several actions to ensure effective access controls, such as requiring office supervisors and data owners to complete Computer System Access forms, requiring users to sign a System Access Agreement, and deleting users' identifications for departing employees. The Mission also said that it would specify required access control actions in its updated Information System Security Plan.

In response to Recommendation No. 1.3, USAID/Egypt said that its Information System Security Plan would include a signed and dated contingency plan. Further, the Mission explained that a contingency site had already been identified, and that it was being prepared.

In regards to Recommendation No. 1.4, the Mission said that its Information System Security Plan would include procedures to ensure that computer security controls operate as intended and are systematically evaluated. The Mission explained that such procedures would include conducting annual mandatory security training, management reviews of event logs, and periodic reviews to ensure that access to different platforms is valid and authorized.

Based on the Mission's comments, including the actions it has already taken to address general control weaknesses and its plan to complete an updated Information System Security Plan, a management decision has been made on Recommendation No. 1.

**Scope and  
Methodology****Scope**

Our audit of USAID/Egypt's information systems' general controls identified and tested controls over the Mission's computer-processing environment. These controls included security program planning and management, access controls, application software and development, segregation of duties, system software, and service continuity plans.

We conducted the audit in accordance with generally accepted government auditing standards. Our fieldwork was conducted at USAID/Egypt between May 30 and August 1, 2001. The audit scope included:

- Reviewing a computer security risk assessment that was performed at USAID/Egypt in August 1999.
- Interviewing cognizant Mission officials.
- Reviewing USAID/Egypt's self-evaluation of its fiscal year 2000 management controls.
- Reviewing the Computer Security Act of 1987 and OMB Circular A-130 as well as Chapters 545 and 552 of USAID's Automated Directives System, which address Automated Information Systems Security and Classified Information Systems Security, respectively.

**Methodology**

We used the General Accounting Office's Federal Information System Controls Audit Manual, Volume I Financial Statement Audits to evaluate USAID/Egypt's information systems' general controls. This Manual divides general controls into six critical elements: (1) a security program, (2) access controls, (3) application software development and change controls, (4) segregation of duties, (5) system software, and (6) service continuity. Appendix III describes each element.

We identified and reviewed the Mission's general control policies and procedures and documented the extent to which USAID/Egypt implemented the controls. Through discussions with officials from the Mission's Management Office, including the Acting Systems Manager, we noted what controls existed. We then tested and observed the operation of controls to determine if they were designed and operating effectively.

MANAGEMENT  
COMMENTS

**USAID**



UNITED STATES AGENCY for INTERNATIONAL DEVELOPMENT



CAIRO, EGYPT

December 31, 2001

Memorandum

To: RIG/Cairo, Darryl Burris  
From: Deputy Director, USAID/Egypt, Anne Aarnes//Signed//  
Subject: Audit of USAID/Egypt's Information Systems' General  
Computer Controls - Draft Report

This memorandum provides USAID/Egypt's comments on the above-referenced draft audit report.

As detailed below, USAID/Egypt is committed to implement an Information Systems Security (ISS) Program to secure the Mission's computer network. The ISS program will also incorporate our action plan for the specific areas described in the referenced audit report. The current status of these areas include:

Plot 1A off El-Laselki Road  
New Maadi  
Cairo, Egypt

Recommendation No. 1: We recommend that USAID/Egypt develop a computer security program that includes:

1.1 developing and maintaining an information systems security plan;

The Mission started developing an updated ISS Plan in accordance with USAID Automated Directives System (ADS) Chapter 545 and OMB Circular No. A-130 to make sure that all the findings will come to closure by July 2002.

The updated plan will be completed by December 1, 2002 and will identify who owns the computer resources and establish a security management structure.

1.2 Implementing effective access controls:

The Mission has already implemented the actions listed below to ensure effective access controls of the computer network and will specify these required actions in the updated ISS plan:

- Data Management Services (DMS) now requests a Computer System Access form to be completed by office supervisors and data owners to assure that the access granted is on a need to know basis.
- Users are required to sign a System Access Agreement form accepting to abide by this agreement to process unclassified information based on established federal and USAID policies prior to gaining access to the network.
- Access to system software is being limited to authorized system software specialists, as evidenced by our system administration password list.

- DMS is deleting users' IDs for departing employees upon signing the departure check-list.
- DMS is using system utilities (e.g. Windows 2000/NT Events Log, Windows 2000 Performance Monitoring) to monitor system status/performance and system events.
- Remote access is being granted only upon documented justification and approval.

**1.3 Preparing and testing an information systems contingency plan:**

The updated ISS plan will include a signed and dated contingency plan specifying the following required actions, which the Mission has already taken:

- The Mission has identified a contingency site and is preparing the location.
- Backup tapes are stored offsite in the warehouse in a protected safe on a weekly basis, and accounting data backups on a daily basis.
- The new contingency plan will identify responsibilities assigned to personnel, and include detailed instructions for data recovery.

**1.4 Monitoring and evaluating the effectiveness of its security program:**

The updated ISS plan will include the procedures outlined below, which USAID/Egypt has already taken, to ensure that computer security controls are operating as intended and to systematically evaluate the Mission's computer security program:

- DMS conducts annual mandatory security training.

- DMS is implementing management reviews and monitoring reports from resources such as the event logs.
- An authorized access list with emergency contacts is posted on the entrance of the computer room.
- Segregation of duties will be addressed in the new DMS organization chart and updated position descriptions.
- Periodic reviews performed by the IT manager ensure that access to different platforms is valid and authorized.
- Periodic self-assessments are conducted to test the security effectiveness and to validate the security controls to ensure proper implementation.

In summary, USAID/Egypt agrees on the necessity of implementing effective controls to secure its information and will perform the necessary actions to implement the recommendation found in the draft audit report.

In view of the above, Mission believes that a management decision has been made and requests resolution of Recommendation No. 1 upon issuance of the final audit report.

Distribution:

OD/SCS, D. McCloud  
OD/FM, H. Jamshed  
OD/LEG, P. Weisenfeld  
A/OD/MGT, M. Sampson  
CIO/MGT/ICT, T. Starks  
A/OD/PROC, R.Plucknet

**GAO's  
Categorization of  
General Controls**

No.	Critical Elements	Description
1.	Security Program	Provides the framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.
2.	Access Controls	Limits or detects access to computer resources. Thus, these controls protect the resources from unauthorized modification, loss, and disclosure.
3.	Application Software Development and Change Controls	Prevents unauthorized programs or modifications to an existing program from being implemented.
4.	Segregation of Duties	Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations.
5.	System Software	Limits and monitors access to the powerful programs and sensitive files that (1) control the computer hardware, and (2) secure applications supported by the system.
6.	Service Continuity	Ensures that, when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

**Detailed Listing  
of Audit Findings**

**Entity-Wide Security Program**

- The Mission's Security Plan was not signed or dated, did not establish a security management structure, did not establish who owned various computer resources, and did not include the expected behavior for all individuals with access to the system or the consequences of behavior not consistent with the rules.
- The Mission did not have an adequate computer security awareness program. That is, the Mission distributed documents describing security policies, procedures, and individual responsibilities, but it did not provide information security orientation, training, or periodic refresher programs to both new and existing employees.
- The Mission did not actively monitor the effectiveness of its information security program to determine whether controls were operating as intended or whether the program was raising awareness levels and reducing security incidents.

**Access Controls**

- Computer access authorization was not documented on standard forms or approved by senior managers.
- There was no periodic review of the access authorization listing to determine whether inappropriate access had been removed in a timely manner. Six of 14 employees, who had left the Mission between December 2000 and June 2001, still had access to the Mission's computer system.
- USAID/Egypt's computer system had a built in function that allowed for the logging of all events occurring in the system, but these logs were not reviewed.
- Justification for granting dial up access to users was not documented.
- Laptop checkout spreadsheet was not always up-to-date.

**Service Continuity**

- The Mission's contingency plan was not signed or dated and did not identify a backup information processing facility, emergency procedures, including assigned responsibilities, or detailed instructions for data recovery.
- Contingency computer equipment and excess computer equipment (some in non-working condition) were mixed together in the Mission's warehouse.
- The Mission's contingency plan had not been tested.