

Regional Inspector General for Audit
Cairo, Egypt

Audit of USAID/Egypt's Security Controls
for the Wang VS as They Relate to MACS

Report No. 6-263-93-04
February 18, 1993





**UNITED STATES OF AMERICA
AGENCY FOR INTERNATIONAL DEVELOPMENT
OFFICE OF THE REGIONAL INSPECTOR GENERAL/AUDIT**

February 18, 1993

MEMORANDUM FOR Director USAID/Egypt, Henry H. Bassford

FROM : RIG/A/C, Philippe L. Darcy

SUBJECT: Audit of USAID/Egypt's Security Controls for the Wang VS
as They Relate to MACS

Enclosed are ten copies of our audit report on USAID/Egypt's Security Controls for the Wang VS as They Relate to MACS, Audit Report No. 6-263-93-04. The report contains two recommendations. We consider Recommendation No. 1 closed and Recommendation No. 2 resolved. Recommendation No. 2 can be closed when we have received a Memorandum of Understanding between USAID/Egypt and the American Embassy in Cairo regarding back-up data processing services.

In finalizing this report, we fully considered your comments on the draft report and have included them as Appendix II to this report. Furthermore, in accordance with your request, we have included the full text of your written representations as Appendix V to this report.

Please provide a response to this report within 30 days indicating what further actions you have taken to address the open recommendation.

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

U.S. Mailing Address
USAID-RIG/A/C Unit 64902
APO AE 09839-4902

Tel. Country Code (202)
357-3909

106, Kasr El Aini St.
Cairo Center Building
Garden City, Egypt

Background

In 1988, the A.I.D. Office of Information Resources Management (IRM) prepared an Automation Security Guidebook to set forth Agency policies and procedures guiding the activities of all A.I.D. operating expense funded, unclassified, automated systems. The guidebook was designed to serve as a reference for overseas Missions as well as for A.I.D./Washington offices and bureaus engaged in automation activities not under the direct control of IRM. USAID/Egypt uses the Wang VS system to run the Mission Accounting and Control System (MACS). MACS is a computer-based accounting and financial management system. It provides USAID missions with financial data integrity, easy access to accounting data, timely and accurate reporting, management reports and relief from the burden of clerical accounting chores. The computer hardware and software are central components of a system consisting of guidelines, procedures and conventions for recording, analyzing and reporting accounting data.

USAID/Egypt's Wang VS system is operated by the Data Management Services Office, which is organized within the Office of Management. The MACS is used by the Office of Financial Management to record accounting transactions. USAID/Egypt obligated \$791,907,543, committed \$760,935,394, and disbursed \$662,551,873 during fiscal year 1991. Because of this large dollar volume, strong computer controls are necessary to ensure that: the use of resources is consistent with laws, regulations and policies; resources are safeguarded against waste, fraud and misuse; and reliable data are obtained, maintained and fairly disclosed in reports.

Audit Objectives

The Office of the Regional Inspector General for Audit/Cairo conducted an audit of USAID/Egypt's security controls over the Wang VS computer used to safeguard the Mission Accounting and Control System (MACS) to answer the following audit objectives:

Has USAID/Egypt assigned the responsibilities for automation security as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

Does USAID/Egypt maintain physical security measures that safeguard the Wang VS system as suggested in A.I.D.'s

Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

Is USAID/Egypt using the Wang VS security system to protect information resources against unauthorized use as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

Has USAID/Egypt performed risk analysis and developed an adequate contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

The audit was designed to provide reasonable assurance in answering the audit objectives and was limited to identifying and testing computer operations controls which were applied to all computer applications. These controls included the assignment of responsibility for computer security, physical controls over computer resources, access controls to computer programs and data, and planning for disaster recovery.

Audit Findings

Based upon discussions with Mission officials, the Director, USAID/Egypt, provided us a written representation that the Mission is responsible for the internal control system and the fairness and accuracy of the accounting and management information relating to the audited activities and that, to the best of his knowledge and belief, USAID/Egypt had provided us all the financial and management information relating to the audit objectives, USAID/Egypt is unaware of any material instances where the information provided had not been properly and accurately recorded and reported, and USAID/Egypt has complied with all contractual agreements that could materially affect the Mission's security controls for the Wang VS computer as they relate to MACS. (The complete representation is contained in Appendix II of this report.)

Although the Director, USAID/Egypt, provided us these essential written representations, he did not provide acceptable representations as to whether he is aware of any instances of irregularities, noncompliance with A.I.D. policies and procedures or violations, or possible violations, of laws and regulations for the activities under audit. Instead, the Director confirmed that, to the best of his knowledge and belief, the records under audit should contain any instances of irregularities or noncompliance or violations. Also, in

accordance with A.I.D./Washington guidance of May 13, 1992, the Mission policy is that only the Director will sign a letter of representation. Therefore, other USAID/Egypt officials directly responsible for the audited activities -- the Director of the Data Management Services Office and the Associate Mission Director for Management -- did not provide written representations confirming essential information. As a result, our answers to the audit objectives are qualified to the extent of the effect of not having such representations.

Has USAID/Egypt assigned the responsibilities for automation security as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

USAID/Egypt assigned the responsibilities for automation security as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government. USAID/Egypt designated the Data Management Services (DMS) Office Director, who is the System Manager, as the System Security Officer for managing and implementing the automated information system security program. This follows the policy prescribed by A.I.D.'s Automation Security Guidebook that each overseas mission with an automated information system designate an American employee to be the Systems Security Officer. The Office Director of DMS reports to the Associate Director for Management who reports directly to the Deputy Mission Director. This organizational scheme provides the System Manager with a reporting mechanism which is independent of the major users of computer resources. It also separates the responsibility for operating computer resources from the responsibility for recording accounting transactions and certifying payments which are performed by the Financial Management Division. Therefore, this organizational structure complies with the "specific" Standard for Internal Controls in the Federal Government addressing separation of duties.

Does USAID/Egypt maintain physical security measures that safeguard the Wang VS system as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

USAID/Egypt maintains physical security measures that safeguard the Wang VS system as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government. However, controls protecting against fire and unauthorized access to the computer facility need strengthening.

The central unit of USAID/Egypt's Wang VS system is a pair of Wang VS100

minicomputers with 12 disk drives and 2 tape drives located in the computer room. We observed the following controls protecting this equipment:

- no ground level windows;
- a location apart from possible hazards such as water pipes;
- two air conditioners to maintain an appropriate temperature;
- a master power shut-off switch; and
- clean electric power provided by uninterruptable power supply equipment.

Even though USAID/Egypt has established controls to safeguard the physical security of the Wang VS system, security could further be enhanced if controls protecting against fire damage and unauthorized access to the computer facility were strengthened.

Controls Over Fire And Access Need Improvement

GAO Standards and the A.I.D. Automation Guidebook require that Mission's establish controls to protect A.I.D. resources. For most facilities, controls protecting personnel and equipment from fire hazards and restricting access to authorized individuals are especially crucial. The audit found that controls protecting the computer facility against fire and unauthorized access were weak. As a result, USAID/Egypt faced increased risk of undetected fire, including the ensuing potential for human and property loss, and unauthorized access to computer facilities. We believe this occurred because (1) the Mission relied on the landlord to test the alarm system, which was rarely done, (2) the Mission did not insist its contractor install cables properly, and (3) locks securing the computer room were inadequate.

Recommendation No. 1: We recommend the Director USAID/Egypt develop an action plan to address the risks posed by infrequent testing of the computer facility smoke detection system, the tangle of cables accessing the Wang VS computer, and the inadequate cipher locks on computer room doors.

GAO's Standards for Internal Controls in the Federal Government require that controls be established to protect U.S. Government resources from loss or unauthorized use. This requirement is evident in A.I.D.'s Automation Security Guidebook which requires that System Managers' install fire sensors (ie. smoke detectors) so fire hazards may be dealt with promptly. Such controls also include those restricting access to U.S. Government computer equipment such as securing computer rooms with combination cipher locks, using badges for visitors, and having procedures for allowing maintenance personnel to enter facilities.

USAID/Egypt faced increased risk of fire because it did not control the upkeep and testing of the computer facility's smoke alarm system and a fire hazard was posed by the array of cables accessing the computer facility. Instead of installing its own smoke detection system, the Mission relied on a system maintained by its landlord. This system, however, does not significantly lower the risk of loss since it is not tested on a regular basis. Additional risk is posed since the tangle of cables accessing the computer room block access to computer connections and outlets. In our opinion, continuous contact and weight of these cables increase the risk that cable insulation will fail, thereby exposing unshielded cables carrying high voltage electricity. Such risk was realized recently when a DMS employee received a severe electrical shock while working among these cables. This condition contrasts with the description of another Mission provided by an A.I.D. official. In this other Mission, computer cables enter the Wang VS computer through a board segregating the cables by Mission office and have labels indicating to where they connect.

As shown in the following photographs, the Mission has taken corrective action to reduce the risk posed by the tangled cables entering the computer room.



**This Tangle of Cables Connected to the Wang VS 100
Minicomputer was a Fire and Electrical Hazard
USAID/Egypt Computer Room October 1992**



**Wang VS 100 Minicomputer Cables
After the Mission's Corrective Action
USAID/Egypt Computer Room January 1993**

The Mission's risk of unauthorized access is increased by the type of combination cipher locks controlling entry to USAID/Egypt's computer facility. We believe an unauthorized person might gain access to the computer room by deciphering the combination locks. The Embassy's Regional Security Officer (RSO) confirmed that USAID/Egypt's current cipher locks represent security risks.

Interviews conducted with a responsible A.I.D. official indicated that USAID/Egypt personnel did not know why the Mission had chosen to rely on the landlord's smoke detection system or why cables accessing the Wang VS computer had become so tangled. While we believe that relying on the landlord's smoke detection system avoided unnecessary costs, it was only logical as long as the landlord ensured that the system was maintained in good working order. The problem is that the landlord seldom tests the smoke detection system and without regular testing to ensure proper operation, the risk of loss of human life and property is increased. We also believe that the Mission's tangled computer cables resulted from accepting substandard work from contractors.

The responsible A.I.D. official indicated that a prior RSO had recommended the currently used combination locks. We believe that these locks were acceptable when recommended because, at the time, a twenty-four hour U.S. Marine security guard presence was maintained at USAID/Egypt. Currently at night, the Mission is only protected by local security guards.

In conclusion, it is crucial that the risk of fire hazard and unauthorized access be minimized to protect against the loss of life and government property. These risk increased with regards to the Mission's computer facility because the smoke detection system was not tested regularly, cables accessing the Wang VS posed a fire hazard, and computer center locks were not adequate. The Mission needs to remedy these problems.

Is USAID/Egypt using the Wang VS security system to protect information resources against unauthorized use as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

USAID/Egypt's System Administrator uses the Wang VS security system to protect information resources against unauthorized use as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government.

The Wang VS security software provides three levels of access controls to safeguard programs and data maintained on the system: (1) user identifications and passwords are required for all users; (2) log-on procedures or programs may be assigned to users to limit their access to specific programs; and (3) file protection classes can be assigned to limit access to specific files.

As suggested in A.I.D.'s Automation Security Guidebook, the System Administrator and her deputy created user identifications for the Wang VS security software. This identification is stored on the system in a users list file which the system employs to authenticate users when they log on. This control reduces the risk of non-authorized individuals accessing the Wang VS system.

Once the system validates a user's identification and password, it will determine whether the user has a log on procedure. This procedure is a series of codes processed automatically by the system, which is specific to a user and which results in a menu allowing access to certain programs. For example, only the staff of the Financial Management Division are assigned menus that allow them to establish obligations in MACS. This control prevents unauthorized users from initiating an obligation in the accounting system.

Each file on the system may be assigned to one (and only one) specified file protection class, which is indicated by a one-character file class code. The System Administrator may establish up to 26 file classes and assign files to each class in a logical manner. Users are subsequently allowed or denied access to file classes and allowed or denied modes of data access (read, execute or write). For example, USAID/Egypt's System Administrator has assigned access to MACS files to file classes accessible to the staff of the Financial Management Division. Only certain Financial Management personnel have write access to these classes of files. This prevents unauthorized users from accidentally or maliciously altering accounting records and conforms to the file protection class and access privilege procedures suggested in A.I.D.'s Automation Guidebook.

In addition to the above standard Wang VS security features, USAID/Egypt recently installed an Enhanced Systems and Access Control (ESAC) program. This program complements the Wang VS security system by adding such features as password encryption, the locking of user identifications after five unsuccessful access attempts and automatic assignment of random eight character passwords by the system every twelve weeks. These and other enhanced security controls provide USAID/Egypt with an extra measure of protection against persons gaining unauthorized access to the system and enhanced compliance with the "specific" Standard for Internal Controls in the Federal Government addressing access to resources.

Has USAID/Egypt performed risk analysis and developed an adequate contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government?

Mission Management has performed risk analysis and developed an adequate contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government. However, we did find that written agreements between USAID/Egypt and the management of alternate processing sites did not exist, disaster recovery plan coverage was too general and regular tests of the disaster recovery plan were not conducted.

USAID/Egypt has performed an analysis of the risk of losing their automated information resources. As suggested in A.I.D.'s Automation Guidebook, their analysis identified likely threats that might disrupt or destroy their computer operations and determined which of their systems were critical to Mission operations. They have also implemented controls to expedite a rapid recovery from any disruption of these systems. For example, USAID/Egypt has a system for producing back-up copies of critical systems on a daily basis. These back-up copies are stored outside of the Wang VS computer center. Weekly back-up copies of critical systems are stored at the American Embassy, Cairo. This off-site storage reduces the chances of both original computer data and back-up data being destroyed by the same disaster.

Although Mission Management has identified likely threats to their computer operations and implemented procedures for backing up computer files, no written agreements between USAID/Egypt and the management of alternate processing sites regarding recovery activities have been established, disaster recovery plan coverage is too general, and regular tests of the disaster recovery plan are not conducted.

Recovery Implementation Can Be Enhanced

A.I.D.'s Automation Security Guidebook and GAO Standards require that Missions establish controls to reduce the risk of loss. Such controls related to disaster recovery include back-up processing agreements, specific actions to be taken during recovery, and controls ensuring that recovery plans are workable and up to date. Our audit found that USAID/Egypt's recovery controls could be improved. In our opinion, this condition resulted from the Mission's not recognizing the importance of these controls whose absence could result in valuable time being lost trying to arrange for necessary resources and by people waiting for instructions in implementing the recovery process.

Recommendation No. 2: We recommend that the Director USAID/Egypt establish written agreements with management of back-up processing sites, modify the written recovery plan to include step-by-step instructions for restoring computer operations for each alternate processing site and for each type of disaster identified in the risk assessment, and test the disaster recovery plan on a regular basis.

A.I.D.'s Automation Security Guidebook notes that contingency/recovery plans should include back-up processing agreements with other agencies or companies having similar facilities. The guidebook also states that the plan should address various levels of threats or disasters and contain specific actions to be taken in each case. GAO's Standards for Internal Control in the Federal Government also require that agencies establish controls to reduce the risk of losing valuable resources. We believe testing of a recovery plan is such a control because it confirms that persons involved understand their responsibilities and that the plan is workable.

Our audit found that USAID/Egypt had not established written agreements with alternate processing sites to be used for data processing during the Mission's recovery from a disaster. In our opinion, without such written agreements neither party has a clear understanding of their respective rights and responsibilities during disaster recovery. The Mission had also not defined specific action steps for recovery in its recovery plan, as required by A.I.D.'s Automation Guidebook. The incorporation of actions steps in the recovery plan is essential because such detail identifies the minimum actions to be taken, the proper sequence of actions, and how recovery is to be achieved. Finally, USAID/Egypt had not complied with GAO Standards by testing its disaster recovery plan.

While the causes for not having a written agreement and not testing the recovery plan were not evident, it is likely that the Mission simply did not recognize the importance of these controls. As a result, we believe USAID/Egypt faces increased risk of losing the use of valuable Agency resources to an unsuccessful or protracted recovery process.

SCOPE AND METHODOLOGY

Scope

We audited USAID/Egypt's security controls over the Wang VS system as related to MACS. The audit covered security applications and procedures in place during the audit field work from February 1992 through October 1992. We conducted our audit in accordance with generally accepted government auditing standards for performance audits, except as discussed below with regard to the extent of representations made by Mission officials.

Government auditing standards require auditors to obtain representation letters when they deem the letters useful. The Office of the Inspector General deems them necessary evidence to support potentially positive findings. We requested USAID/Egypt's management to furnish a written representation regarding this audit assignment. Based on discussions with Mission officials, USAID/Egypt's Director provided us a written representation that USAID/Egypt is responsible for the internal control system and the fairness and accuracy of the accounting and management information relating to the audited activities and that, to the best of his knowledge and belief, USAID/Egypt had provided us all the financial and management information relating to the audit objectives. USAID/Egypt is unaware of any material instances where the information provided had not been properly and accurately recorded and reported, and USAID/Egypt has complied with all contractual agreements that could materially affect the Mission's security controls for the Wang VS computer. (The complete representation is contained in Appendix II of this report.)

Although the Director, USAID/Egypt, provided us these essential written representations, he did not provide acceptable representations as to whether he is aware of any instances of irregularities, noncompliance with A.I.D. policies and procedures or violations, or possible violations, of laws and regulations for the activities under audit. Instead, the Director confirmed that, to the best of his knowledge and belief, the records under audit should contain any instances of irregularities or noncompliance or violations. Also, in accordance with A.I.D./Washington guidance of May 13, 1992, the Mission policy is that only the Director will sign a letter of representation. Therefore, other USAID/Egypt officials directly responsible for the audited activities -- the Director of the Data Management Services Office and the Associate Mission Director for Management -- did not provide written representations to the Director confirming essential information. As a result, our answers to the audit objectives are qualified to the extent of the effect of not having such representations.

In performing our audit, we reviewed organization charts, job descriptions, Wang VS reports, DMS documents, and USAID/Egypt's disaster recovery plan. We verified this evidence through interviews, physical observations, and consulting the Regional Security Officer.

The audit did not cover the following areas because they were outside the audit scope:

- Application controls of the Mission Accounting and Control System (MACS);
- Application controls of the Mission Accounting and Control System Voucher Tracking System (MACSTRAX); and
- Controls within the Office of Financial Management.

The audit was limited to identifying and testing computer operations controls which were applied to all computer applications. These controls included the assignment of responsibility for computer security, physical controls over computer resources, access controls to computer programs and data, and planning for disaster recovery.

Methodology

The methodology for each audit objective follows.

Audit Objective One

The first audit objective was to determine if USAID/Egypt assigned responsibilities for automation security as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government.

To accomplish this audit objective, we discussed current security practices with security officials and prepared an organizational chart identifying operational responsibilities for security controls for the security of the Mission's Wang VS hardware and software. We also identified the relevant security controls in place and determined whether they followed the guidance of the A.I.D. Automation Security Guidebook and the "specific" Standards for Internal Controls in the Federal Government. Finally, we reviewed mission policies that supported the independence of the information systems function.

We tested the system functions for proper segregation of duties. This involved:

- Reviewing published organizational charts to determine whether they allowed for separation of duties and functions.
- Interviewing selected members of the information systems staff to determine whether their duties and responsibilities corresponded to the published position description and the organizational chart.

Audit Objective Two

The second objective was to determine if USAID/Egypt maintains physical security measures that safeguard the Wang VS system as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government.

To accomplish this audit objective, we examined physical and environmental control procedures and compared them with the guidance in A.I.D.'s Automation Security Guidebook. We toured the computer facilities to determine their security strengths and weaknesses.

We also examined how easily one could access the computer room. In this regard, we observed the type of locking equipment, access policies regarding maintenance personnel and whether unauthorized individuals were challenged when entering the proximity of the computer area.

We determined whether the computer facility was protected by fire control smoke detection equipment. We questioned whether the activation of detection equipment resulted in an audible alarm in the computer room as well as in another centrally located site.

Audit Objective Three

The third objective was to determine if USAID/Egypt uses the Wang VS security system to protect information resources against unauthorized use as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government.

To accomplish this objective, we interviewed information system personnel to determine what type of information system security software had been installed in the system.

We examined the supervision and use of passwords and other access codes and symbols. This examination included:

- Reviewing procedures for eliminating a password when an employee resigns or is terminated.
- Reviewing the Users' Attribute Listing to determine if access to MACS and MACSTRAX applications programs and data were consistent with job responsibilities.

Audit Objective Four

The fourth objective was to determine if USAID/Egypt performed risk analysis and developed an adequate contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government.

To accomplish this objective, we determined if a risk assessment had been performed on the vulnerability of the Wang VS system. Further, we determined whether the risk assessment:

- Identified likely threats;
- Calculated the value of threatened resources; and
- Prioritized critical applications to be restored in the event of disruption.

We examined the contingency strategy planning process and determined whether provisions had been made to address impact areas, including:

- Backup of critical hardware, software and data;
- Specific responsibilities for executing the contingency plan;
- Procedures for notifying key personnel; and
- Specific actions to be taken for each type of identified likely threat.

We visited off-site back-up tape storage locations and assessed whether security and environmental controls were adequate. We also reviewed procedures for backing up critical data.

**MANAGEMENT COMMENTS
AND OUR EVALUATION**

USAID/Egypt's response to the draft report is included in its entirety in this appendix. The Mission has also requested that its letter of audit representations be included as part of its comments. Therefore, this letter is also included in Appendix V. The Mission's response to the draft report and the actions it proposes to implement the recommendations are discussed below, as well as our response to the Mission's comments.

- Recommendation No. 1 - The Mission developed an action plan to address risk of fire in and unauthorized access to the computer room. We consider the recommendation closed based on this plan.
- Recommendation No. 2 - USAID/Egypt has included both action steps in its written disaster recovery plan and the requirement for an annual test of recovery procedures. The Mission is also discussing the establishment of a Memorandum of understanding (MOU) with the Embassy regarding access to back-up data processing facilities. We consider the recommendation resolved. We will close this recommendation upon execution of the MOU.



CAIRO, EGYPT

UNITED STATES AGENCY for INTERNATIONAL DEVELOPMENT

APPENDIX II

Page 2 of 5

RECEIVED
31 JAN 1993

MEMORANDUM

JAN 28 1993

TO: Philippe A. Darcy, RIG/A/C

FROM: Douglas S. Franklin, AD/FM *DSF*

SUBJECT: Draft Report on Audit of USAID.Egypt's Security Controls for the Wang VS as They Relate to MACS - Draft Report Dated December 9, 1992

In reviewing the draft audit report and its recommendations, USAID/Egypt has undertaken several actions to address potential risks endangering data, property, or staff as mentioned in the subject audit. Following is the Mission's response to the two recommendations under the subject draft audit report:

Recommendation No. 1:

We recommend the Director USAID/Egypt develop an action plan to address the risks posed by infrequent testing of the computer facility smoke detection system, the tangle of cables accessing the Wang VS computer, the gap between the top of the computer room walls and the actual ceiling, and the insufficient cipher locks on the computer room doors.

Mission Response:

The AID Automation Security Guidebook requires the Mission to take reasonable measures to protect the computers and data. This has been accomplished. The following measures to safeguard the security of the computer systems and data are in place:

- 1) Maintenance contract for core VS equipment ensures that all parts can be repaired or replaced;
- 2) Daily backups of all systems and data;
- 3) Weekly data and system backups are stored off-site;
- 4) All contractor staff with access to core computer equipment or wiring maintain security clearances and after-hours access approval;

13

- 5) Enhanced security software locks-out anyone who tries to illegally access files and records attempts to violate the system;
- 6) The computer room is located behind the hard line and protected by two doors with cipher locks whose combinations are changed every six months;
- 7) The computer room is designed so that both doors and the room itself are visible to Data Management staff.

Regarding fire detection, management has temporarily installed a smoke detector, but will use the forthcoming visit of an AID/Washington security team to obtain a recommendation for an alarm for the computer room which will be connected with the security guard. The landlord's detector will be disconnected because it has not been made operable after multiple requests from management to repair it.

Until USAID staff no longer need VS minicomputer data processing programs, it will be necessary to continue using the coaxial cable. Coax use has been minimized by the Local Area Network, particularly for electronic mail.

Coax cabling does not constitute a fire hazard because it carries very low voltage. There are no special high voltage electrical wires entering the computer room. Wiring is the same voltage used to power regular office equipment.

However, coax laying on some electrical cables powering VS and Network equipment, has caused an exposed wire to be pulled from the wall shocking a DMS Operator. To address this situation, during December 1992 the coaxial cabling was organized by port, labeled per device, tied and placed in trays beneath the false floor of the computer room. This separates coax from electrical cabling and eliminates the possibility of disconnecting or exposing a wire when heavy pieces of coax are pulled. Further, VS drive cables were also re-organized, and replaced where needed. This will expedite diagnosis of system problems and separate all cabling to the maximum extent possible.

Deleted - Relates to Matter Not Included in Final Report

Cipher locks in place are adequate and do not need to be replaced. The locks were originally selected by the Embassy Regional Security Office, as required by the AID Automation Security Guidebook. Removal of the Marine Guard on the ninth floor does not constitute an indication of an increased physical security risk; if anything, it reflects a lowered security risk for the Mission. The Data Management Services office is unaware of any increased technological risks. Given that the VS system contains no classified data and that controls are in place to recover equipment and data, investment in vault-type protection is not warranted at this time.

However, to ensure that after-hours entry into the computer room by authorized staff is monitored and unauthorized access deterred, the Mission will install a contact sensor on the outside door of the computer room with a phone line connected to Marine Post One at the Embassy. This alarm will be enabled when the last DMS employee leaves for the day; it will be disabled when the DMS employee contacts Post One to resume work. The addition of the contact sensor strengthens the overall security of the Wang VS and substantially reduces the risks identified in the gap between the top of the computer walls and the actual ceiling and the cypher locks on the computer room doors.

We believe that the above Mission action plan is more than adequate and is the most cost-effective to address the risks identified in the recommendation. Based on the above action, Mission requests that Recommendation No. 1 be closed.

Recommendation No. 2:

We recommend that the Director USAID/Egypt establish written agreements with management of back-up processing sites, modify the written recovery plan to include step-by-step instructions for restoring computer operations for each alternate processing site and for each type of disaster identified in the risk assessment, and test the disaster recovery plan on a regular basis.

Mission Response:

USAID/Egypt's risk assessment and contingency plan discusses potential threats, the response to different types of threats, and possible approaches for recovery.

System failures force Data Management Services to practice recovery procedures about once per month. The Mission believes that a full test of disaster recovery procedures during normal working hours is not cost-effective because it would result in loss of data. For the Mission Accounting and Control System (MACS), simulating a system crash during normal business hours would result in additional data entry and report creation for a large number of Financial Management staff; as such it could delay payment to vendors and grantees and have a negative effect on payroll.

We have added to our Disaster Plan the recommendation to test recovery procedures once per year. As discussed in the Risk Assessment, the Embassy is USAID/Egypt's primary alternate site for both technical and security reasons. To avoid loss of data and excessive downtime for Mission users, USAID/Egypt plans to test CPU 2 system recovery once per year on a weekend or government holiday. This will involve scheduling at least 2-3 days per year, overtime for both Embassy and USAID staff. (See the Disaster Recovery Implementation Plan, attached). The Disaster Recovery Plan has been updated, providing additional detail on recovery procedures (See Attached Plan). Names are not assigned to tasks because: a) with a tape or disk back-up of a system or data, plus the user list, most operators and programmers could install the applications and data; and b) in the event of an emergency such as civil war or an earthquake, it is unlikely that all staff would be able to travel safely to Cairo Center or the Embassy.

USAID/Egypt and the Embassy have an agreement to support each other's data processing requirements in the event of an emergency. The Mission concurs that having such an agreement in writing can facilitate implementation of emergency procedures should force majeure close either of the computer centers. A Memorandum of Understanding on using each other's facilities for emergency processing has been discussed with the Embassy Administrative Counselor. The MOU is being prepared. Based on the above, Mission requests this recommendation be resolved. Mission will request closure when the MOU is signed.

21

REPORT ON INTERNAL CONTROLS

This section provides a summary of our assessment of USAID/Egypt's internal controls for the audit objectives.

Scope of Our Internal Control Assessment

Based upon discussions with Mission officials, the Director, USAID/Egypt, provided us a written representation that the Mission is responsible for the internal control system and the fairness and accuracy of the accounting and management information relating to the audited activities and that, to the best of his knowledge and belief, USAID/Egypt had provided us all the financial and management information relating to the audit objectives, USAID/Egypt is unaware of any material instances where the information provided had not been properly and accurately recorded and reported, and USAID/Egypt has complied with all contractual agreements that could materially affect the Mission's security controls for the Wang VS computer as they relate to MACS. (The complete representation is contained in Appendix II of this report.)

Although the Director, USAID/Egypt, provided us these essential written representations, he did not provide acceptable representations as to whether he is aware of any instances of irregularities, noncompliance with A.I.D. policies and procedures or violations, or possible violations, of laws and regulations for the activities under audit. Instead, the Director confirmed that, to the best of his knowledge and belief, the records under audit should contain any instances of irregularities or noncompliance or violations. Also, in accordance with A.I.D./Washington guidance of May 13, 1992, the Mission policy is that only the Director will sign a letter of representation. Therefore, other USAID/Egypt officials directly responsible for the audited activities -- the Director of the Data

22'

Management Services Office and the Associate Mission Director for Management -- did not provide written representations confirming essential information. As a result, our conclusions on the internal controls are qualified to the extent of the effect of not having such representations.

Except for the above, we performed our work according to generally accepted government auditing standards for performance audits which require that we (1) assess the applicable internal controls when necessary to satisfy the audit objectives and (2) report on the controls assessed, the scope of our work, and any significant weaknesses found during the audit.

We limited our assessment of internal controls to those controls applicable to the audit's objectives and not to provide assurance on the auditee's overall internal control structure.

We categorized significant internal control policies and procedures applicable to each audit objective. For each category, we obtained an understanding of the design of relevant policies and procedures and determined whether they have been placed in operation--and we assessed control risk. We have reported these categories as well as any significant weaknesses under the applicable section heading for each audit objective.

The categories used are the six "specific" Standards for Internal Control as defined by the General Accounting Office (GAO).

General Background on Internal Controls

Under the Federal Managers' Financial Integrity Act and the Office of Management and Budget's implementing policies, A.I.D.'s management is responsible for establishing and maintaining adequate internal controls. The General Accounting Office has issued "Standards for Internal Controls in the Federal Government" to be used by agencies in establishing and maintaining internal controls.

The categories we used are the six "specific" standards for internal control as defined by the GAO in "Standards for Internal Controls In The Federal Government." The internal control standards define the minimum level of quality acceptable for internal control systems in operation and constitute the criteria against which systems are to be evaluated.

A number of techniques are essential to providing the greatest assurance that the internal control objectives will be achieved. These critical techniques are the specific standards discussed below.

1. **Documentation.** Internal control systems and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination.
2. **Recording of Transactions and Events.** Transactions and other significant events are to be promptly recorded and properly classified.
3. **Execution of Transactions and Events.** Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.
4. **Separation of Duties.** Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.
5. **Supervision.** Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.
6. **Access to and Accountability for Resources.** Access to resources and records is to be limited to authorized individuals, and accountability for the custody and use of resources is to be assigned and maintained. Periodic comparison of the resources shall be made with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

The objectives of internal controls and procedures are to provide management with reasonable--but not absolute--assurance that resource use is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data is obtained, maintained, and fairly disclosed in reports.

Because of inherent limitations in any internal control structure, errors or irregularities may occur and not be detected.

Predicting whether a system will work in the future is risky because (1) changes in conditions may require additional procedures or (2) the effectiveness of the design and operation of policies and procedures may deteriorate.

Conclusions for Audit Objective 1

The first objective was to determine if USAID/Egypt assigned responsibilities for automation security suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government. To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the Federal Government. We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective.

Except for the effects, if any, of not receiving acceptable representations, as discussed above in the Scope of Our Internal Control Assessment, our tests showed that the internal controls were logically and consistently applied.

Conclusions for Audit Objective 2

The second objective was to determine if USAID/Egypt maintains physical security measures that safeguard the Wang VS System suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the Federal Government. To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the Federal Government. We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective.

Our tests showed that the internal controls were logically and consistently applied except for the effects, if any, of not receiving acceptable representations, as discussed above in the Scope of Our Internal Control Assessment, and for the following weaknesses.

- The smoke alarm system protecting the computer facility is not tested regularly.
- Tangled cables entering and exiting the computer room pose a fire hazard, in our opinion.
- Cipher locks controlling computer room access are inadequate.

Conclusions for Audit Objective 3

The third objective was to determine if USAID/Egypt uses the Wang VS Security System to protect information resources against unauthorized use suggested in A.I.D.'s Automation Security Guidebook and "specific" Standards for Internal Controls in the Federal Government. To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the Federal Government. We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective.

Except for the effects, if any, of not receiving acceptable representations, as discussed above in the Scope of Our Internal Control Assessment, our tests showed that the internal controls were logically and consistently applied.

Conclusions for Audit Objective 4

The fourth objective was to determine USAID/Egypt performed risk analysis and developed an adequate contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" GAO's Standards for Internal Controls in the Federal Government. To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the Federal Government. We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective.

Our tests showed that the internal controls were logically and consistently applied except for the effects, if any, of not receiving acceptable representations, as discussed above in the Scope of Our Internal Control Assessment, and for the following weaknesses.

- No written agreements exist concerning alternate processing sites.
- USAID/Egypt's recovery plan does not contain specific action steps.
- The disaster recovery plan has not been tested.

REPORT ON COMPLIANCE

This section summarizes the auditor's conclusions on USAID/Egypt's compliance with applicable laws and regulations.

Scope of Compliance Assessment

We audited USAID/Egypt's security controls over the Wang VS system as related to MACS. The audit covered security applications and procedures in place during the audit field work from February 1992 through October 1992. We conducted our audit in accordance with generally accepted government auditing standards for performance audits, except as discussed below with regard to the extent of representations made by Mission officials.

Government auditing standards require auditors to obtain representation letters when they deem the letters useful. The Office of the Inspector General deems them necessary evidence to support potentially positive findings. We requested USAID/Egypt's management to furnish a written representation regarding this audit assignment. Based on discussions with Mission officials, USAID/Egypt's Director provided us a written representation that USAID/Egypt is responsible for the internal control system and the fairness and accuracy of the accounting and management information relating to the audited activities and that, to the best of his knowledge and belief, USAID/Egypt had provided us all the financial and management information relating to the audit objectives. USAID/Egypt is unaware of any material instances where the information provided had not been properly and accurately recorded and reported, and USAID/Egypt has complied with all contractual agreements that could materially affect the Mission's security controls for the Wang VS computer. (The complete representation is contained in Appendix II of this report.)

21'

Although the Director, USAID/Egypt, provided us these essential written representations, he did not provide acceptable representations as to whether he is aware of any instances of irregularities, noncompliance with A.I.D. policies and procedures or violations, or possible violations, of laws and regulations for the activities under audit. Instead, the Director confirmed that, to the best of his knowledge and belief, the records under audit should contain any instances of irregularities or noncompliance or violations. Also, in accordance with A.I.D./Washington guidance of May 13, 1992, the Mission policy is that only the Director will sign a letter of representation. Therefore, other USAID/Egypt officials directly responsible for the audited activities -- the Director of the Data Management Services Office and the Associate Mission Director for Management -- did not provide written representations to the Director confirming essential information. As a result, our answers to the audit objectives are qualified to the extent of the effect of not having such representations.

Except for the above, we conducted our audit in accordance with generally accepted government auditing standards which require that we:

- (1) assess compliance with applicable requirements of laws and regulations when necessary to satisfy the audit objectives (which includes designing the audit to provide reasonable assurance of detecting abuse and illegal acts that could significantly affect the audit objectives) and
- (2) report all significant instances of noncompliance and abuse and all indications or instances of illegal acts that could result in criminal prosecution that were found during or in connection with the audit.

General Background on Compliance

Noncompliance is a failure to follow requirements, or a violation of prohibitions, contained in statutes, regulations, contracts, grants, and binding policies and procedures governing entity conduct. Noncompliance constitutes an illegal act when there is a failure to follow requirements of laws or implementing regulations, including intentional and unintentional noncompliance and criminal acts. Not following internal controls policies and procedures in the A.I.D. Handbooks generally does not fit into this definition of noncompliance, and is included in our report on internal controls. Abuse is distinguished from noncompliance in that abusive conditions may not directly violate

laws or regulations. Abusive activities may be within the letter of the law but violate either its spirit or the more general standards of impartial and ethical behavior.

Compliance with laws and regulations applicable to computer security is the overall responsibility of USAID/Egypt's management.

Conclusions on Compliance

As management was not willing to confirm in a representation letter essential information related to compliance with applicable laws and regulations, we cannot therefore state positively that USAID/Egypt has complied.



UNITED STATES AGENCY for INTERNATIONAL DEVELOPMENT

CAIRO, EGYPT

RECEIVED
28 OCT 1992

Mr. Philippe L. Darcy
Regional Inspector General
for Audits
Cairo, Egypt

OCT 27 1992

Dear Mr. Darcy:

This Representation Letter is being issued in accordance with Agency guidance in response to the audit of "USAID/Egypt's Security Controls for the Wang VS as they Relate to MACS" recently conducted by your Staff.

Based upon discussions with Mission Staff, and taking into account identified staffing constraints and vulnerabilities as expressed in Mission ICAs, to the best of my knowledge and belief, I confirm that all appropriate financial records in the possession and under the control of USAID/Cairo relating to the function being audited have been made available to you. To the best of my knowledge and belief, the records made available to you are accurate and complete, and they fairly represent the status of Security Controls for the Wang VS as they Relate to MACS within the Mission. To the best of my knowledge and belief, in conjunction with the confirmation in A, B, C and D below, those records, and verbal representations of AID employees currently in the Mission, should have identified any instances of non-compliance or irregularities, or violations of laws and regulations as those terms may be defined by or perceived by the Inspector General. Specifically I confirm that:

- (A) USAID/Egypt is responsible for the internal control system, for the fairness and accuracy of accounting and management information for the function under audit. USAID/Egypt to the best of my knowledge and belief exercises its best efforts to ascertain and follow applicable U.S. laws and AID regulations and AID interpretations of those laws and regulations.

30

- 2 -

- (B) To the best of my knowledge and belief, and based on discussions and verbal representations by others in the Mission, USAID/Egypt has made available to you or otherwise provided you at your request all financial and management information related to the audit objectives.
- (C) To the best of my knowledge and belief, except for any findings or other matters included in the audit report, USAID/Egypt is unaware of any material instances associated with the function being audited where financial or management information has not been properly and accurately recorded/reported.
- (D) To the best of my knowledge and belief, USAID/Egypt has complied with all contractual agreements, to the extent there are such agreements, which could have any material effect on Mission Security Controls for the Wang VS as they Relate to MACS.

Upon review of your draft report and following further discussion with my staff, I know of no events subsequent to the date of your draft report, (other than those which were included in our response to that report), which to the best of my knowledge and belief would materially alter the statements in (A) thru (D) above.

All representations made herein by me are made in light of my experience since my arrival at post.

I request that this Representation Letter be included as a part of the official management comments on the draft report and that it be published therewith as an Annex to the report.

Sincerely yours,


Henry H. Bassford
Director

31

REPORT DISTRIBUTION

	<u>No. of Copies</u>
U.S. Ambassador to Egypt	1
Mission Director, USAID/Egypt	10
Assistant Administrator for Bureau for Near East, AA/NE	1
Associate Administrator for Finance and Administration, AA/FA	1
Associate Administrator for Operations, AA/OPS	1
Audit Liaison Office for Near East	1
Office of Press Relations, XA/PR	1
Office of Financial Management, FA/FM	1
AA/R&D	1
Bureau for Legislative Affairs, LEG	1
Office of the General Counsel, GC	1
POL/CDIE/DI, Acquisitions	1
FA/MCS	2
FA/FM/FPS	2
IG	1
AIG/A	1
IG/A/PPO	3
IG/LC	1
AIG/I&S	1
IG/RM	12
Other RIG/A's	1 each