

PD-ABE-206
78

Regional Inspector General for Audit
Nairobi, Kenya

Audit of
USAID/Yemen's Security of the Wang VS
as Related to MACS

Report No. 3-279-92-10
May 29, 1992



U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

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

UNITED STATES POSTAL ADDRESS
BOX 232
APO N.Y. 09875

INTERNATIONAL POSTAL ADDRESS
POST OFFICE BOX 30261
NAIROBI, KENYA

May 29, 1992

MEMORANDUM

TO: George Flores, Director, USAID/Yemen

FROM: Joseph Farinella, Acting/RIG/A/Nairobi

SUBJECT: Audit of USAID/Yemen's Security of the Wang VS as Related to MACS



Enclosed are five copies of our audit report on USAID/Yemen's Security of the Wang VS as Related to MACS, Report No. 3-279-92-10.

We were not able to fully answer the audit objectives because USAID/Yemen's management declined to provide us with all the information essential for us to render a professional conclusion. These scope limitations will be discussed in more detail in the body of the report.

We have reviewed your comments on the draft report and included them as an appendix to this report. The first recommendation is closed upon report issuance and all others are resolved and will be closed when appropriate actions are completed. Please respond to this report within 30 days indicating any actions planned to implement the recommendations.

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

EXECUTIVE SUMMARY

Background

The Office of Information Resources Management (M/SER/IRM) plans, develops, procures and supports all automated systems in the Agency for International Development (A.I.D.). IRM prepared an Automation Security Guidebook to set forth A.I.D. automated policies and procedures to serve as a reference for overseas missions. Through Fiscal Year 1990, the USAID/Yemen's Controller's Office had obligated \$ 3.4 million, committed \$ 2.3 million, and expended \$ 2.2 million for agricultural and educational activities (see pages 1 and 2).

Audit Objectives

We audited USAID/Yemen's Security of the Wang VS as related to MACS in accordance with generally accepted government auditing standards (see page 2 and Appendix I). Our field work was conducted from October 1, 1991 through October 10, 1991 to answer the following audit objectives:

1. Has USAID/Yemen 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 (see page 6)?
2. Does the System Administrator maintain physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government (see page 7)?
3. Is the System Administrator 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 (see page 10)?
4. Has USAID/Yemen performed a risk analysis and developed a 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 (see page 13)?

Summary of Audit

We were unable to fully answer the audit objectives because USAID/Yemen's management would not provide us with a written confirmation that, to the best of their knowledge and belief: (1) all essential information was provided to us, (2) the information provided was accurate and complete, and (3) management had followed A.I.D. policies. In view of the above, this report is limited because we cannot state positively that USAID/Yemen followed A.I.D. policies and procedures applicable to the audit objectives (see page 5). However we are able to report that certain procedures were not followed: (1) the combination on the computer room door was not changed on a periodic basis putting \$80,000 worth of equipment vulnerable to potential misuse and destruction (see page 8); (2) passwords were not changed to ensure authorized access to resources (see page 10); and (3) contingency plans were not developed and documented to protect software, equipment and the data files in the event that the equipment would not operate (see page 13).

Audit Findings

Responsibilities for Automation Security

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether USAID/Yemen 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.

Maintenance of Physical Security Measures

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether the Systems Administrator maintains physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by the General Accounting Office's (GAO) "specific" Standards For Internal Controls In The Federal Government. However, we are able to report the following problem area which came to our attention:

Combination on the Computer
Room Door Should be Changed

The Automation Security Guidebook states that information center door combinations must

be changed at intervals not to exceed six months. Also, the General Accounting Office's (GAO) specific standard for "Access to and Accountability for Resources" requires that access to resources and records be limited to authorized individuals. However, at the time of the audit, USAID/Yemen had not changed the combination on the computer room door for close to a year and a half. This occurred because USAID/Yemen was not aware of the requirement to change the combination every six months. As a result, current safeguards did not ensure against unauthorized access to the computer room by individuals who could misuse and destroy equipment valued at approximately \$80,000 (see page 8).

Protection of Information Resources Against Unauthorized Use

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether the System Administrator was 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 the General Accounting Office's (GAO) "specific" Standards For Internal Controls In The Federal Government. However, we are able to report the following problem area which came to our attention:

Password Administration Should be Improved

GAO's specific standards on "Access to and Accountability for Resources" and "Documentation" require that access to resources and records is to be limited to authorized individuals and that internal controls be documented. The Automation Security Guidebook states that security software should fully implement the systems security features and that passwords should be changed every three months. However, the security software in use by USAID/Yemen did not completely ensure authorized access to the Wang VS System and passwords were not changed every three months. This occurred because A.I.D./Washington advised USAID/Yemen to minimize additional software and hardware purchases for the Wang VS system and Automated Data Processing (ADP) security at the Mission had not been given priority in relation to the other administrative, financial and project tasks within the Mission. As a result, current safeguards did not ensure against unauthorized access by individuals who could destroy, change or otherwise manipulate data (see page 10).

Performance of Risk Analysis and Contingency Planning

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether USAID/Yemen performed a risk analysis and developed a contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by the General Accounting Office's "specific"

Standards For Internal Controls In The Federal Government. However, we are able to report the following problem area which came to our attention:

**Contingency Plans Were
Not Developed and Documented**

GAO's specific standard on "Documentation" requires that internal control systems, all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination. However, USAID/Yemen did not document contingency or disaster recovery plans for its automated information resources and did not have procedures for developing and documenting contingency plans. This occurred because USAID/Yemen was not aware of the requirement to document such procedures. As a result, contingency plans were not developed and documented to protect software, equipment valued at \$80,000 and the data files in the event that the equipment would not operate (see page 13).

Summary of Recommendations

This report contains three recommendations to correct the problem areas noted above. We recommend that the Director, USAID/Yemen:

- ensure that the combination on the computer room door is changed at least every six months (see page 8);
- establish written procedures and upgrade security software (see page 11); and
- develop and publish contingency plans (see page 14).

Management Comments and Our Evaluation

USAID/Yemen reviewed the draft report and agreed with the findings and recommendations (see Appendix II).

Office of the Inspector General

Office of the Inspector General
May 29, 1992

Table of Contents

	Page
EXECUTIVE SUMMARY	i
INTRODUCTION	
Background	1
Audit Objectives	2
REPORT OF AUDIT FINDINGS	5
1. Has USAID/Yemen 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?	6
2. Does the System Administrator 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?	7
The combination on the computer room door should be changed	8
3. Is the System Administrator 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?	10
Password Administration should be improved	10
4. Has USAID/Yemen performed a risk analysis and developed a 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?	13
Contingency plans were not developed and documented	13
REPORT ON INTERNAL CONTROLS	16
REPORT ON COMPLIANCE	21
	<u>Appendix</u>
SCOPE AND METHODOLOGY	I
MANAGEMENT COMMENTS	II
REPORT DISTRIBUTION	III

INTRODUCTION

Background

The Office of Information Resources Management (M/SER/IRM) plans, develops, procures and supports all automated systems in the Agency for International Development (A.I.D.). IRM prepared an Automation Security Guidebook to set forth A.I.D. policies and procedures to guide all operating expense funded activities, unclassified A.I.D./Washington automated projects and programs, and overseas automated systems. The guidebook is designed to serve as a reference for overseas missions, and for offices and bureaus in A.I.D./Washington engaged in automation activities not under the direct control of M/SER/IRM.

Where applicable, sections of the Automation Security Guidebook were derived from government documents, such as the Office of Management and Budget's Circular A-130 and the National Security Decision Directive 145.

The Mission Accounting and Control System (MACS) is a computer-based accounting and financial management system. MACS consists of data stored in computer files, computer programs, processing control rules, and procedures governing the interface between accounting personnel and the computer system itself. The computer hardware and software are situated at the center of an environment made up of guidelines, procedures, and conventions for recording, analyzing and reporting accounting data within USAID missions.

Through Fiscal Year 1990, the USAID/Yemen's Controller's Office had obligated \$ 3.4 million, committed \$ 2.3 million, and expended \$ 2.2 million on agricultural and educational development support activities. A strong computer security system is needed to ensure that resource use is consistent with laws, regulations and A.I.D. policies; that resources are safeguarded against waste, fraud and misuse; and that reliable data are obtained, maintained, and fairly disclosed in reports.

The Computer Security Act of 1987, Public Law 100-235, was enacted on January 8, 1988. The Act requires that all federal agencies identify their computer systems, whether operational or under development, that contain sensitive information. The act also requires

agencies to establish security plans for each identified system, and establish training programs to increase security awareness and knowledge of security practices.

Audit Objectives

The Office of the Regional Inspector General for Audit/Nairobi conducted an audit of USAID/Yemen's Security of the Wang VS as related to MACS to answer the following audit objectives:

1. Has USAID/Yemen 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?
2. Does the System Administrator maintain physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government?
3. Is the System Administrator 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?
4. Has USAID/Yemen performed a risk analysis and developed a 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?

Our review was made in accordance with generally accepted government auditing standards for performance audits and accordingly included such tests of the accounting records and other auditing procedures as we considered necessary in the circumstances. Our tests were sufficient to provide reasonable--but not absolute--assurance that our answers to the audit objectives are valid.

However, when we found problem areas, we performed additional work to:

- identify the cause and effect of the problems and

- make recommendations to correct the condition and cause of the problems.

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

REPORT OF AUDIT FINDINGS

We are not able to fully answer our audit objectives because USAID/Yemen's management declined to provide us all the information essential for us to render a professional conclusion.

For example, USAID/Yemen's management would not confirm that to the best of their knowledge and belief:

- they had provided us with all the essential information,
- the information they did provide to us was accurate and complete, and
- they had followed A.I.D.'s policies.

(A complete description of the essential information that USAID/Yemen would not provide or confirm is provided in the Scope and Methodology section of this report.)

Without these confirmations from USAID/Yemen, we cannot fully determine if USAID/Yemen did what it is required to do. Without such confirmations, we would, in essence, be stating that USAID/Yemen complied with A.I.D.'s policies and procedures when USAID/Yemen itself is unwilling to make such a statement.

While we cannot state positively that USAID/Yemen followed its policies and procedures, this lack of a management confirmation would not preclude us from reporting on any problem areas that came to our attention. Based on the information that USAID/Yemen did provide to us and the tests that we were able to perform, the following information came to our attention.

1. Has USAID/Yemen 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?

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether USAID/Yemen 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.

A.I.D.'s Automation Security Guidebook states that, at overseas posts, it is A.I.D. policy that an American direct-hire employee will serve as the Mission's Systems Security Officer. In addition, the General Accounting Office's "specific" standards for "Supervision" and "Separation of Duties" state that qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved, and that key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

In line with the above guidelines, USAID/Yemen's records showed that the system's security function is assigned to the controller, an American direct-hire employee. Reporting to the controller and independent from other accounting functions and activities, is the systems manager, who is responsible for overseeing the day-to-day operations of the automated system at USAID/Yemen, including security related activities.

Management Comments and Our Evaluation

USAID/Yemen did not comment on this audit objective in its response to our draft report.

2. Does the System Administrator maintain physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government?

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether the Systems Administrator maintains physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by the General Accounting Office's (GAO) "specific" Standards For Internal Controls In The Federal Government. However, we are able to report the following problem area which came to our attention:

- The combination on the computer room door should be changed.

The Automation Security Guidebook suggests that all automated systems should be kept in a secure and in an environmentally controlled facility to protect them from fire and water damage. The facility should also provide adequate weight-bearing floors, meet temperature and power requirements, and have sufficient space to allow for entry, installation, and maintenance of equipment.

In addition, GAO's specific standard for "Access to and Accountability for Resources" states that 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. Further, periodic comparison shall be made of the resources with the recorded accountability to determine whether the two agree.

Mission officials stated that all Wang VS-related equipment at USAID/Yemen is kept in a secure, environmentally controlled facility and appropriate controls were in place within the computer facility to protect equipment, materials and employees against fire or water hazards.

According to USAID/Yemen's records, the Systems Administrator maintained an inventory system of Wang VS-related equipment by model number, serial number and location. This would be in line with the specific standard for "Access to and Accountability for Resources." Mission documentation showed that computer hardware and related equipment were accounted for. However, we found that the combination on the computer room door was not changed on a regular basis as discussed below.

**Combination on the Computer
Room Door Should be Changed**

The Automation Security Guidebook states that information center door combinations must be changed at intervals not to exceed six months. Also, as noted above GAO's specific standard for "Access to and Accountability for Resources" requires that access to resources and records is limited to authorized individuals. However, at the time of the audit USAID/Yemen had not changed the combination on the computer room door in close to a year and a half. This occurred because USAID/Yemen was not aware of the requirement to change the combination every six months because they did not give ADP security a high enough priority. As a result, current safeguards did not ensure against unauthorized access to the computer room by individuals who could destroy equipment valued at approximately \$80,000, or otherwise change or manipulate data.

Recommendation No. 1: We recommend that the Director, USAID/Yemen:

- 1.1 issue a Mission Order requiring that the combination on the computer room door be changed at least every six months and that the changes be documented by the Controller or a person designated by him or her; and**
- 1.2 report the internal control weakness, associated with not changing the combination on the computer room door, to the Assistant Administrator in the next annual Federal Managers' Financial Integrity Act reporting cycle if this weakness is not corrected.**

The Automation Security Guidebook states that information center door combinations must be controlled and changed as necessary--at intervals not to exceed six months. GAO's specific standard on "Access to and Accountability for Resources" requires that access to resources and records be limited to authorized individuals.

USAID/Yemen had not changed the combination on the computer room door since it was installed at the beginning of April 1990, almost a year and a half prior to the audit.

USAID/Yemen did not change the combination on the computer room door because they were not aware of: (1) the provision in the Automation Security Guidebook to change the combination on the computer room door at least every six months, and (2) GAO's specific standard on the "Access to and Accountability for Resources" which requires that access to resources and records be limited to authorized individuals. This lack of awareness also occurred because Automated Data Processing (ADP) security had not been given priority in relation to the other administrative, financial and project tasks within the Mission.

Further, computer room personnel did not know how to change the combination on the cipher lock since they were inexperienced in doing so.

As a result, the potential existed for an unauthorized person to enter the computer room and gain access to change or otherwise manipulate data files or cause damage and destruction to computer equipment valued at approximately \$80,000.

Based on the foregoing, we concluded that USAID/Yemen needed to issue a directive to increase awareness to emphasize the importance of ADP security, including the need to follow prescribed procedures.

Management Comments and Our Evaluation

In its response to our draft report, the Mission agreed with our conclusion and recommendation. Management stated that the combination to the computer room door has been changed and that a mission directive has been issued (Order No. 15-1 dated October 22, 1991) which requires that the cipher lock combination be changed at least every six months and that the changes be documented.

The cited action by the Mission closes the recommendation upon report issuance.

3. Is the System Administrator 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?

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether the System Administrator was 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 the General Accounting Office's (GAO) "specific" Standards For Internal Controls In The Federal Government. However, we are able to report the following problem area which came to our attention:

- Password administration should be improved.

The Automation Security Guidebook states that the systems manager is responsible for establishing logon user IDs and passwords for VS minicomputers. In addition, the systems manager should control the addition and deletion of users or revision of access rights. Specifically, passwords should be deleted when an individual is no longer employed with the Mission. Further, engineers may be issued a logon ID and password only when required to perform service and the password should be changed upon completion of the service call.

GAO's specific standards on "Access to and Accountability for Resources" and "Documentation" also states that access to resources is to be limited to authorized individuals and that internal controls be documented.

The Wang VS user's list provided by the Mission showed that only current employees were on it. Moreover, passwords are only issued to customer service engineers when required and are changed at the end of each service call. Also, according to the systems administrator, the customer service engineers are escorted at all times when he or she are on the mission's premises.

However, as discussed below, password administration did not completely assure against unauthorized access to the Wang VS System.

**Password Administration
Should be Improved**

GAO's specific standards on "Access to and Accountability for Resources" and "Documentation" requires that access to resources and records is to be limited to authorized individuals and that internal controls be documented. The Automation Security Guidebook

states that security software should fully implement the systems security features and that passwords should be changed every three months. However, the security software in use by USAID/Yemen did not completely assure against unauthorized access to the Wang VS System and passwords were not changed every three months. This occurred because A.I.D./Washington advised USAID/Yemen to minimize additional software and hardware purchases for the Wang VS system and the Systems Administrator did not ensure that passwords were changed every three months because Automated Data Processing (ADP) security had not been given priority in relation to the other administrative, financial and project tasks within the Mission. As a result, current safeguards did not ensure against unauthorized access by individuals who could destroy, change or otherwise manipulate data.

Recommendation No. 2: We recommend that the Director, USAID/Yemen:

- 2.1 establish written procedures and upgrade security software to ensure that passwords are changed every three months; and**
- 2.2 report the internal control weakness, associated with not changing passwords every three months and the vulnerability of the software, to the Assistant Administrator in the next annual Federal Managers' Financial Integrity Act reporting cycle if this weakness is not corrected.**

GAO's specific standard on "Access to and Accountability for Resources" requires that 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. Similarly, GAO's specific standard on "Documentation" requires that 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. The Automation Security Guidebook states that security software should fully implement the operating systems security features and that passwords should be changed and new ones issued every three months.

USAID/Yemen uses the Wang VS Security Utility Version 7.20.08 software. Although the Mission had implemented all of the security utility's features, the software does not completely assure against unauthorized access to the Wang VS System. For example, the software does not have the capability of: (1) encrypting passwords; (2) locking out a violator of the system after a specified number of improper access attempts; (3) monitoring unauthorized or improper access attempts for subsequent review and action by USAID/Yemen; and (4) setting automatic expiration dates for user passwords. The systems administrator stated that a sophisticated user could, if he or she had access to the computer room, bypass current security checks and gain unauthorized access to system files. As such,

USAID/Yemen had contemplated improving password administration which included the purchase of additional security software. However, the Mission did not change passwords every three months, nor did it document the internal control procedure to do so.

USAID/Yemen did not improve password administration by purchasing upgraded software because A.I.D. Information Resource Management discouraged missions from purchasing new Wang hardware or software because of the Agency's move towards microcomputer-based systems. USAID/Yemen did not change passwords at three-month intervals nor did it document the internal control procedure to do so because Automated Data Processing (ADP) security had not been given priority in relation to the other administrative, financial and project tasks within the Mission. During the audit, USAID/Yemen agreed that upgrading software (at an estimated cost of \$3,000) and changing passwords every three months would enhance Automated Data Processing security.

As a result of not having the foregoing safeguards, unauthorized individuals could gain access to the system and destroy, change or otherwise manipulate data which would involve time and effort to restore it from the last back-up.

Thus, we concluded that the Mission should improve password administration by ensuring that the Systems Administrator requires passwords to be changed every three months and that a record be maintained of these changes. Furthermore, USAID/Yemen should also establish written procedures and upgrade its security software.

Management Comments and Our Evaluation

In its response to our draft report, USAID/Yemen agreed with our conclusions and recommendation. Management provided us with a copy of a mission directive which requires passwords to be changed every three months. USAID/Yemen has informed RIG/A/N that they have requested IRM, AID/W to purchase upgraded security software.

The cited actions are responsive to the recommendation. The recommendation is therefore resolved upon report issuance and will be closed upon receipt by this office of a copy of the purchase order for the security software.

4. Has USAID/Yemen performed a risk analysis and developed a 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?

As discussed on page five, because of the limitations placed on the audit by management, we are unable to report whether USAID/Yemen performed a risk analysis and developed a contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by the General Accounting Office's "specific" Standards For Internal Controls In The Federal Government. However, we are able to report the following problem area which came to our attention:

- Contingency plans were not developed and documented.

A.I.D.'s Automation Security Guidebook states that risk analysis and contingency planning for automated information resources should be accomplished by each mission. Further, one of the risks that should be assessed is to determine the value of each information resource that is threatened and compare this with the cost of protecting it.

Documentation provided by the Mission showed that USAID/Yemen, in conjunction with Information Resource Management, performed a vulnerability assessment of USAID/Yemen's computer facility in March 1990. This assessment identified the mission's automation equipment as being vulnerable because there were no locks on the computer room door, the room was not dust-proof, there were no smoke alarms and there was only one hand-held fire extinguisher. The report stated that immediate attention should be given to the facility.

During a tour of the computer room, the systems administrator showed us that the Mission had acted upon the report's findings. For example, he showed us two doors that had been installed in the computer room facility, one with a cipher lock and the other to reduce the amount of dust in the computer room. In addition, a smoke detector and two fire extinguishers had been installed.

However, as discussed below, USAID/Yemen did not develop nor document its ADP contingency plans.

**Contingency Plans Were
Not Developed and Documented**

The Automation Security Guidebook states that the Systems Security Officer should develop

and document a step by step contingency plan and recovery process. In addition, GAO's specific standard on "Documentation" requires that internal control systems, all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination. However, USAID/Yemen did not document contingency or disaster recovery plans for its automated information resources and did not have procedures for developing and documenting contingency plans. This occurred because USAID/Yemen was not aware of the requirement to document such procedures and it did not assign ADP security high enough priority in relation to the other administrative, financial and project tasks within the Mission. As a result, contingency plans were not documented to protect software, equipment valued at \$80,000 and data files in the event that the equipment would not operate.

Recommendation No. 3: We recommend that the Director, USAID/Yemen:

- 3.1 develop and publish contingency plans for its automated information resources; and**
- 3.2 report the internal control weakness, associated with not developing and publishing contingency plans, to the Assistant Administrator in the next annual Federal Managers' Financial Integrity Act reporting cycle if this weakness is not corrected.**

The Automation Security Guidebook states that the Systems Security Officer should develop a step-by-step contingency plan and recovery process which should be integrated into the overall emergency plan of the Mission. The plan should address various levels of threat or disaster and contain specific actions to be taken in each case. In addition, GAO's specific standard on "Documentation" requires that internal control systems, all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination.

USAID/Yemen did not develop and publish contingency and disaster recovery plans for its automated information resources nor did it report this internal control weakness in its 1990 General Assessment (see page 19).

USAID/Yemen did not develop and document contingency and disaster recovery plans because it was not aware of the requirement for documenting such plans to cover its automated information resources. This lack of awareness resulted from the fact that the Mission did not assign ADP security a high enough priority in relation to the other administrative, financial and project tasks within the Mission. However, USAID/Yemen did successfully transfer its Mission Accounting and Control System processing capability to

A.I.D./Washington in December 1990 as part of the Mission's shut-down and evacuation prior to the start of the Gulf War. As part of the shut-down, personnel also moved ADP hardware to the safe-haven within the mission complex. The successful shut-down and transfer of processing capability to Washington was confirmed by the Mission Director, who at the time of the Gulf Crisis was in charge of coordinating evacuations from the Middle East. The fact that USAID/Yemen successfully evacuated without documented contingency and disaster recovery plans further diminished their perceived need for such plans.

However, without documented plans USAID/Yemen did not have alternative courses of action to protect software, equipment valued at \$80,000 and data files, in the event of different contingencies. Therefore, there was the potential for the disruption of operations at USAID/Yemen by not having access to the data in the event of a contingency.

Thus, we concluded that in order to strengthen contingency and disaster planning, USAID/Yemen needed to develop and document such plans.

Management Comments and Our Evaluation

In its response to our Record of Audit Findings, USAID/Yemen agreed with our conclusions and recommendation. Management provided us with the mission directive that incorporates contingency planning. Further, it stated that it is working with Information Resource Management in A.I.D./Washington to adapt world-wide ADP contingency plans to its mission specific requirements. In its response to our draft report, the Mission stated that it plans to have an ADP contingency plan documented by May 31, 1992 and will forward a copy of the plan to RIG/A/Nairobi.

The cited actions resolve the recommendation upon report issuance. The recommendation will be closed upon receipt by this office of the contingency plan.

REPORT ON INTERNAL CONTROLS

This section provides a summary of our assessment of internal controls for the audit objectives.

We have audited USAID/Yemen's internal controls for the Wang VS Security System for the period October 1, 1989 through September 30, 1990, and have issued our report thereon dated May 29, 1992.

Scope of Our Internal Control Assessment

We conducted our audit in accordance with generally accepted government auditing standards, except that management would not provide us with a representation letter confirming, among other things, its responsibility for the internal controls related to the audit objectives or confirming whether or not there were any instances of noncompliance with A.I.D. policies and procedures or whether or not it had provided us with all the information related to this audit.

Management's refusal to make such representations, constitutes a limitation on the scope of the audit and is sufficient to preclude an unqualified conclusion on the reliability of the internal controls related to the audit objectives. (A complete description of the representations that USAID/Yemen would not make is provided in the Scope and Methodology section of this report.)

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 (GAO) has issued "Standards For Internal Controls In The Federal Government" to be used by agencies in establishing and maintaining internal controls.

The objectives of internal controls and procedures for federal foreign assistance are to provide management with reasonable--but not absolute--assurance that resource use is

consistent with A.I.D. 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.

Explanation of Categories Evaluated

The categories we used are the six specific standards for internal controls defined by 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 operations and constitute the criteria against which systems are to be evaluated.

Specific Standards

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 shall be made of the resources 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.

Conclusions for Audit Objective One

Has USAID/Yemen 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?

We assessed USAID/Yemen's internal controls relating to assigned responsibilities for automation security and the GAO's specific standards for "Supervision" and "Separation of Duties." We are not, however, able to reach a conclusion on the reliability of these controls, as management was not willing to confirm essential information related to these controls in a representation letter.

Because of this lack of management information, we cannot therefore state positively that the internal controls relative to this audit objective are effective and can be relied on. However, based on the information that USAID/Yemen did provide, we can report only that no significant internal control weaknesses came to our attention, other than USAID/Yemen's inability to confirm essential information about its own internal controls.

Conclusions for Audit Objective Two

Does the System Administrator maintain physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government?

We assessed USAID/Yemen's internal controls relating to security measures that safeguard the Wang VS System and the GAO's specific standard for "Access to and Accountability for Resources." We are not, however, able to reach a conclusion on the reliability of these controls, as management was not willing to confirm essential information related to these controls in a representation letter.

Because of this lack of management information, we cannot therefore state positively that the internal controls relative to this audit objective are effective and can be relied on. However, based on the information that USAID/Yemen did provide to us and the tests that

we were able to perform, we can report the following weakness:

- The combination on the computer room door was not changed.

This internal control weakness was not included in USAID/Yemen's 1990 General Assessment nor in the 1988 Assessment of the Controller's Office.

Conclusions for Audit Objective Three

Is the System Administrator 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?

We assessed USAID/Yemen's internal controls relating to the protection of information resources against unauthorized use and the GAO's specific standards for "Access to and Accountability for Resources" and "Documentation." We are not, however, able to reach a conclusion on the reliability of these controls, as management was not willing to confirm essential information related to these controls in a representation letter.

Because of this lack of management information, we cannot therefore state positively that the internal controls relative to this audit objective are effective and can be relied on. However, based on the information that USAID/Yemen did provide to us and the tests that we were able to perform, we can report the following weakness:

- The Mission did not have adequate security software or written procedures to require that passwords are changed every three months.

This internal control weakness was not included in USAID/Yemen's 1990 General Assessment nor in the 1988 Assessment of the Controller's Office.

Conclusions for Audit Objective Four

Has USAID/Yemen performed a risk analysis and developed a 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?

We assessed USAID/Yemen's internal controls relating to risk analysis and contingency planning for its automated resources and the GAO's specific standard for "Documentation." We are not, however, able to reach a conclusion on the reliability of these controls, as management was not willing to confirm essential information related to these controls in a

representation letter.

Because of this lack of management information, we cannot therefore state positively that the internal controls relative to this audit objective are effective and can be relied on. However, based on the information that USAID/Yemen did provide to us and the tests that we were able to perform, we can report the following weakness:

- Contingency plans were not developed and documented.

This internal control weakness was not included in USAID/Yemen's 1990 General Assessment nor in the 1988 Assessment of the Controller's Office.

REPORT ON COMPLIANCE

This section summarizes our conclusions on USAID/Yemen's compliance with the Federal Managers' Financial Integrity Act (FMFIA) as it relates to this audit.

Scope of our Compliance Assessment

We conducted our audit in accordance with generally accepted government auditing standards, except that management would not provide us with a representation letter confirming to the best of their knowledge and belief (1) their responsibility for compliance with applicable laws and regulations, (2) whether or not there were any irregularities involving management or employees, (3) whether or not there were any instances of violations or possible violations of laws and regulations. (A complete description of the representations that USAID/Yemen would not make is provided in the Scope and Methodology section of this report).

Management's refusal to make such representations, constitutes a limitation on the scope of the audit and is sufficient to preclude us from designing our audit to provide reasonable assurance of detecting abuse and illegal acts and from giving an unqualified conclusion on compliance with the Federal Managers' Financial Integrity Act.

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 an organization's conduct. Noncompliance constitutes an illegal act when the source of the requirement not followed or prohibition violated is a statute or implementing regulation, including intentional and unintentional noncompliance and criminal acts. Not following internal control policies and procedures in the A.I.D. Handbooks generally does not fit into the 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 laws and regulations but violate either their spirit or the more general standards of impartial and ethical behavior.

Compliance with the Federal Managers' Financial Integrity Act (FMFIA) is the overall responsibility of A.I.D. which, in turn, requires each Mission to comply with the Act as set forth by binding policies in Department of State Cables sent to Missions each year.

Conclusions on Compliance

We reviewed USAID/Yemen's compliance with the general assessment cable guidance for 1990. As management was not willing to confirm in a representation letter essential information related to such compliance, we cannot therefore state positively that USAID/Yemen complied. However, based on the information that USAID/Yemen did provide to us and the tests that we were able to perform, we can report that USAID/Yemen performed an abbreviated general assessment in 1990 due to the Gulf Crisis and the Mission's evacuation, and that no irregularities or instances of violations of binding policy came to our attention.

SCOPE AND METHODOLOGY

Scope

We followed generally accepted government auditing standards except that USAID/Yemen's management would not provide us with a representation letter (although we requested they provide us one) confirming information essential to fully answer the audit objectives. Management's refusal to make such representations constitutes a limitation on the scope of the audit. The information that USAID/Yemen's management would not confirm, to the best of their knowledge and belief, follows:

1. whether they are responsible for the internal control system, compliance with applicable laws and regulations, and the fairness and accuracy of the accounting and management information for the organization under audit;
2. whether they have provided us with all the financial and management information associated with the activity or function under audit;
3. whether they know of any irregularities in the activity;
4. whether they know of any material instances in which financial or management information has not been properly and accurately recorded and reported;
5. whether they are aware of any instances of noncompliance with A.I.D. policies and procedures or violations of laws and regulations;
6. whether they have complied with contractual agreements; and
7. whether they know of any events subsequent to the period under audit that could affect the above representations.

The answers to the above questions are so fundamental to the basic concepts of auditing that it is not possible to render a positive conclusion without them. Thus, if managers will not answer these basic questions and will not confirm their answers in writing through a representation letter, then we cannot risk giving a positive conclusion when managers will not even confirm to us what they know.

While we cannot render a positive conclusion without such representations, this lack of a management confirmation does not preclude us from reporting on any problem areas that came to our attention and we have done so.

The audit covered the period of October 1, 1989 through September 30, 1990, and reviewed procedures in-place at the time of our field work. The audit field work was conducted from October 1, 1991 through October 10, 1991 in Sana'a, Yemen Arab Republic. We relied on and examined records provided by the Mission, interviewed USAID/Yemen officials and performed a site visit to conduct the audit. However, we did not review any prior audit reports related to Wang VS security as we were unable to find any prior reports on the subject.

Methodology

In addition to the specific methodology followed for each audit objective shown below, we also reviewed USAID/Yemen's 1990 General Assessment in light of the internal control weaknesses identified in the Report on Internal Controls (see page 16). The methodology for each audit objective follows.

Audit Objective One

Has USAID/Yemen 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 answer this audit objective, we obtained an organizational chart to identify operational responsibilities for security controls for the technical and physical security of the mission's hardware and software. We discussed the chart with mission officials to make sure the chart accurately reflects on-going security control practices. We also identified the security control elements and their area of coverage, and determined whether the security elements are adequate to assure data/systems integrity and reliability within its area of coverage.

Next, we reviewed policy statements and related communications from top management which supported the independence of the information systems functions. We determined

whether the security officer conducts systems security training as well as periodic security briefings to all persons with access to the automated systems. We tested the security control elements on the systems users to determine if the users are knowledgeable of security requirements and practices.

We tested the systems functions for proper separation of duties. This involved:

- reviewing published organizational charts for the overall plan of the organization to determine whether it allows for separation of duties and functions; and
- interviewing selected members of the information systems organization to determine that their duties and responsibilities corresponded to the published position description and the organizational chart.

We tested the users responsibility for the protection of information technology systems. This included determining whether the users are:

- monitoring the access to the workstations located in their worksite;
- reporting any abnormal conditions which affect the security of the information system;
- controlling the disposition of output, including using burn bags, shredders, or other means appropriate to the sensitivity of the information; and
- protecting the password by not writing it down, or periodically changing it to avoid easy access by unauthorized individuals.

A major risk associated with security management is that the integrity, confidentiality and the availability of information systems data and resources may be compromised. In this regard, we:

- reviewed and evaluated personnel policies regarding hiring practices, especially procedures for reference and background checks;
- reviewed mandatory requirements regarding employee vacation policies;
- evaluated and tested the procedures for security processing of terminated personnel; and

- reviewed training policies as well as actual training records to determine that personnel are adequately trained in the use of computer systems and technology.

Audit Objective Two

Does the System Administrator maintain physical security measures that safeguard the Wang VS Security System as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government?

To answer this audit objective, we obtained current copies of all logs and record keeping systems maintained by the Systems Administrator to determine if the records were complete and properly maintained and reviewed on a regular basis.

We examined the physical and environmental control procedures and compared them with current policies and future plans. We toured the computer facilities to determine security strengths and weaknesses.

We also examined the ability to access the computer room and systems. In this regard, we observed the type of locking equipment, badge system to allow access, and whether or not outside individuals were challenged when entering the proximity of the computer area and the information systems.

We selected a judgmental sample from the Mission's inventory of Wang VS-related equipment and traced items in the sample by location, model numbers and serial numbers.

We made unannounced visits to the computer area to test whether access control procedures are being followed, and violations recorded. We determined whether the computer facility is protected by zone control smoke detection equipment both above and below the raised floors.

We questioned whether the activation of detection equipment results in an audible alarm outside the computer room and an automatic notification at the nearest fire department. We also questioned whether an alarm system has been installed to alert for unauthorized entry to the computer facility; and is the alarm engaged to alert the authorities.

We reviewed procedures for logging problems to determine that all abnormal hardware and software operating conditions are documented.

Audit Objective Three

Is the System Administrator 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 required by "specific" Standards For Internal Controls In The Federal Government?

To answer this objective, we interviewed information systems personnel to determine the type of information security software installed, and that all significant features of the software were installed and being used. We also determined that there was not a dial-up system in use.

We examined the management and use of the password and other system's access codes or symbols. This included:

- reviewing procedures for changing the password when an employee resigns or is terminated;
- reviewing procedures for authenticating users and issuing new passwords when a user reports that a password has been forgotten or lost; and
- determining whether the security software automatically signs a user off the system if the password is not used within a designated time period.

Improper control procedures over rejected transactions increases the potential for fraud, waste, and abuse. In this regard, we determined whether adequate controls exist over rejected transactions, and that valid transactions are corrected and put back into the system.

Audit Objective Four

Has USAID/Yemen performed a risk analysis and developed a 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 answer this objective, we interviewed mission personnel and reviewed documentation to determine if a risk assessment had been performed on the vulnerability of the Wang VS System.

Further, since the mission had been shut down and direct hire personnel evacuated during the Gulf Crisis, we interviewed mission officials and reviewed documentation to assess the

mission's contingency planning and recovery procedures.

We also visited the off-site storage location and assessed whether security and environmental controls are adequate.

ACTION AIR 5

0000 VZCZSTR049540377
 DE RUEHSN #2519 1241154
 ZNR HUNUU 7ZH
 R 051154Z MAY 92
 FM AMEMBASSY SANAA
 TO AMEMBASSY NAIROBI 0037
 BT
 UNCLAS SANAA 02519

RECEIVED

25-MAY-92

TOR: 12:50
 CHRG: MID
 DIST: AA

6 MAY 92 11 12

USAID/AFYAMA

ATTN: FOR RIG/A/NAISOB, JOSEPH FARINELLA

0000 FROM MISSION DIRECTOR, GEORGE FLORES

E.C. 12356; N/A

SUBJECT: AUDIT OF USAID/YEMEN'S SECURITY OF THE WANG VS
AS RELATED TO MACS

REF: A) FLORES/JARMAN MEMO DATED 10/31/91,
 B) FARINELLA/FLORES MEMO DATED 4/8/92

1. USAID/YEMEN PROVIDED ITS COMMENTS PER REF A TO THE RIG/A/N ON THE RAFS FOR THE SUBJECT AUDIT WHICH HAVE BEEN INCORPORATED IN THE SUBJECT DRAFT AUDIT REPORT UNDER CAPTION "MANAGEMENT COMMENTS AND OUR EVALUATION". HOWEVER, SINCE THEN, THERE HAVE BEEN SEVERAL CHANGES THAT SHOULD BE INCLUDED IN OUR COMMENTS; AND WE REQUEST RIG/A/N TO INCLUDE THEM IN THE FINAL REPORT. THE CHANGES ARE AS FOLLOWS:

2. PAGE 13 OF THE DRAFT AUDIT REPORT UNDER CAPTION "MANAGEMENT COMMENTS AND OUR EVALUATION", PLEASE INSERT IN SECOND SENTENCE AFTER "HAS BEEN ISSUED" "(ORDER NO. 15-1 DATED OCTOBER 22, 1991)". DELETE FINAL SENTENCE IN THIS PARAGRAPH.

A. WE ARE TAKING ACTION TO HAVE THE MASTER POWER SWITCH LOCATED OUTSIDE OF THE COMPUTER ROOM. WE HAVE BEEN UNSUCCESSFUL IN LOCATING A REMOTE SMOKE ALARM SYSTEM AND WOULD APPRECIATE YOUR HELP IN LOCATING THIS ITEM.

B. MISSION BELIEVES THAT NECESSARY ACTION HAS AND IS BEING TAKEN AND RECOMMENDS THAT RECOMMENDATION NO. 1 BE CONSIDERED RESOLVED ON ISSUANCE OF THE AUDIT REPORT.

3. PAGE 18 UNDER CAPTION "MANAGEMENT COMMENTS AND OUR EVALUATION", PLEASE DELETE THE LAST SENTENCE "IN ADDITION THROUGH MARKET" AND INSERT THE FOLLOWING:

"USAID/YEMEN HAS INFORMED RIG/A/N THAT THEY HAVE ALREADY REQUESTED IRM, AID/W, TO PURCHASE UPGRADED SECURITY SOFTWARE. A COPY OF SANAA 02090 IS ENCLOSED."

21

4. BASED ON ABOVE INFORMATION MISSION REQUESTS THAT THE RECOMMENDATION NO. 2 BE CLOSED UPON ISSUANCE.

0000

4. PARAGRAPH - AT THE END OF THE PARAGRAPH, PLEASE INSERT THE SENTENCE "MISSION PLANS TO HAVE AN ADR CONTINGENCY PLAN DOCUMENTED BY 5/31/92 AND WILL FORWARD A COPY OF THE PLAN TO RIC/A/N."

5. MISSION WOULD LIKE TO INFORM RIC/A/N THAT USAID/YEMENS MACS HAS BEEN TRANSFERRED TO USAID/JORDAN EFFECTIVE APRIL 1, 1992, AND JORDAN HAS BEEN DESIGNATED AS THE ACCOUNTING STATION FOR USAID/YEMEN. COPY OF STATE 11518 ATTACHED. STRATHEARN

PT
#2519
NNNN

APPENDIX III

Report Distribution

American Ambassador to Yemen	1
Mission Director, USAID/Yemen	5
AA/ANE	1
ANE/MENA	1
ANE/DP/F	1
XA/PR	1
LEG	1
GC	1
AA/OPS	1
FA/FM	1
AA/FA	1
AA/R&D	1
POL/CDIE/DI	1
FA/MCS	2
FA/FM/FPS	2
REDSO/ESA	1
REDSO/RPMC	1
REDSO/Library	1
IG	1
AIG/A	1
D/AIG/A	1
IG/A/PPO	2
IG/LC	1
IG/RM	12
AIG/I	1
RIG/I/N	1
IG/A/PSA	1
IG/A/FA	1
RIG/A/C	1
RIG/A/D	1
RAO/M	1
RIG/A/S	1
RIG/A/T	1
RIG/A/V	1
RIG/A/EUR/W	1