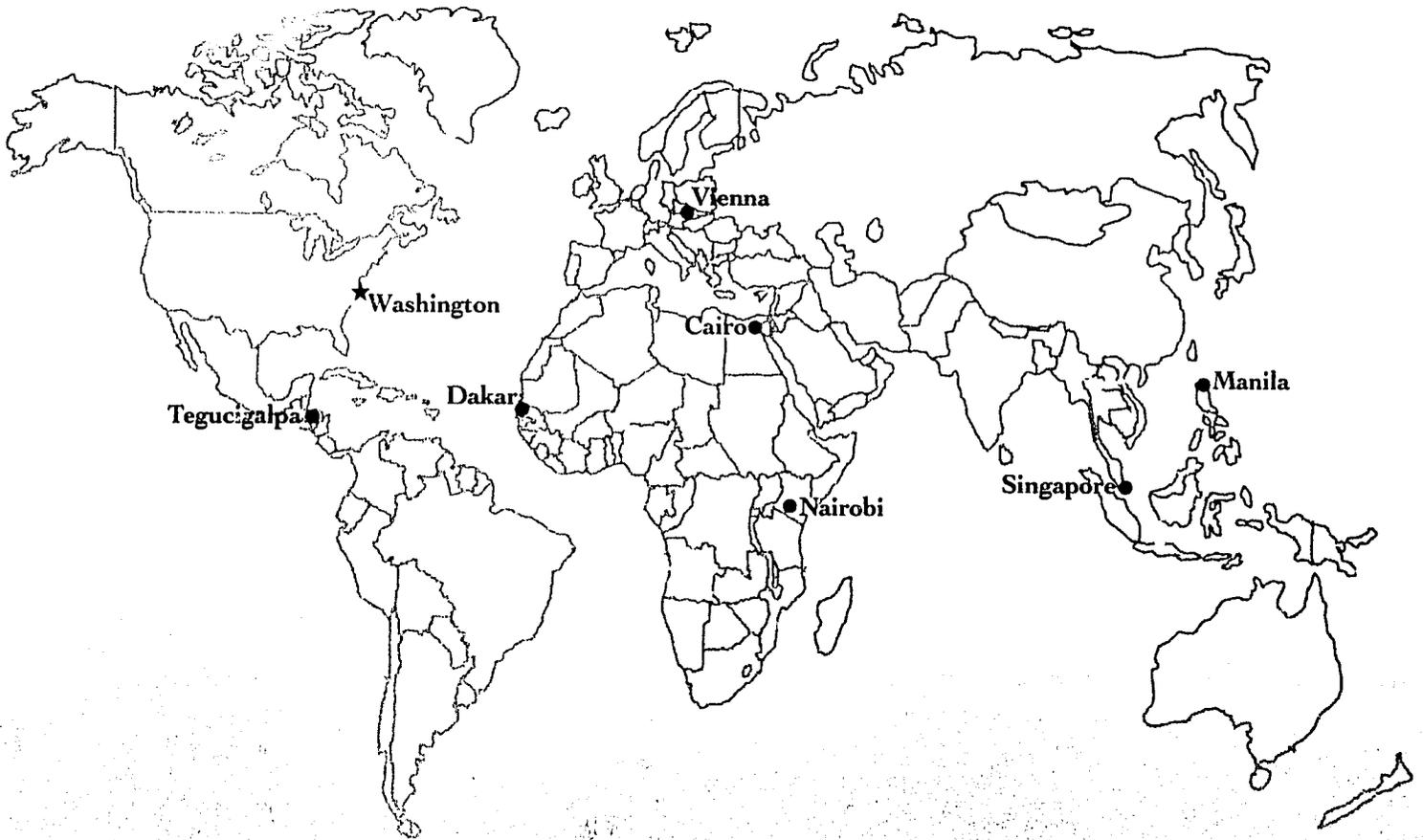


Regional Inspector General for Audit
Nairobi, Kenya

Audit of
USAID/Zimbabwe's Security of the Wang Vs
as Related to MACS

Report No. 3-613-92-13
July 29, 1992



INSPECTOR
GENERAL

U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

UNITED STATES OF AMERICA

AGENCY FOR INTERNATIONAL DEVELOPMENT REGIONAL INSPECTOR GENERAL FOR AUDIT

UNITED STATES POSTAL ADDRESS
UNIT 64102
APO AE 09831-4102

INTERNATIONAL POSTAL ADDRESS
POST OFFICE BOX 30261
NAIROBI, KENYA

July 29, 1992

MEMORANDUM

TO: Ted D. Morse, Director, USAID/Zimbabwe

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

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

Enclosed are five copies of our audit report on USAID/Zimbabwe's Security of the Wang VS as Related to MACS, Report No. 3-613-92-13.

We were not able to fully answer the audit objectives because USAID/Zimbabwe'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. Since there are no recommendations contained in this report, no further action is required by the Mission.

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 the Fiscal Year ended September 30, 1990, the USAID/Zimbabwe Controller's Office had obligated about \$130.1 million, committed \$120.0 million, and disbursed \$112.8 million for active agricultural, basic education and manpower development activities in Zimbabwe (see pages 1 and 2).

Audit Objectives

We audited USAID/Zimbabwe's Security of the Wang VS as Related to MACS in accordance with generally accepted government auditing standards (see Appendix I, page 17). Our field work was conducted from January 7 through January 16, 1992 to answer the following audit objectives:

1. Has USAID/Zimbabwe 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 5)?
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 6)?
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 7)?
4. Has USAID/Zimbabwe performed a 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 (see page 8)?

Summary of Audit

We were unable to fully answer the audit objectives because USAID/Zimbabwe's management would not provide us with a representation letter confirming essential information. In view of the above, this report is limited because we cannot state positively that USAID/Zimbabwe followed A.I.D. policies and procedures applicable to the audit objectives (see page 4).

Audit Findings

Responsibilities for Automation Security

As discussed on page four, because of the limitations placed on the audit by management, we are unable to report whether USAID/Zimbabwe assigned responsibilities for automation security 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, USAID/Zimbabwe's records showed that the system's security function was in line with A.I.D.'s Automation Security Guidebook and GAO's "specific" standards for "Supervision" and "Separation of Duties" (see page 5).

Maintenance of Physical Security Measures

As discussed on page four, 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 GAO's "specific" Standards For Internal Controls In The Federal Government.

However, Mission officials stated that all Wang VS-related equipment at USAID/Zimbabwe is kept in a secure, environmentally controlled facility and appropriate controls were in place to protect and account for equipment and materials (see page 6).

Protection of Information Resources Against Unauthorized Use

As discussed on page four, 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 GAO's "specific" Standards For Internal Controls In The Federal Government.

However, USAID/Zimbabwe's users' list showed that only current employees were on it, in line with A.I.D.'s Automation Security Guidebook and GAO's "specific" standard on "Access to and Accountability for Resources" (see page 7).

Performance of Risk Analysis and Contingency Planning

As discussed on page four, because of the limitations placed on the audit by management, we are unable to report whether USAID/Zimbabwe performed a 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 GAO's "specific" Standards For Internal Controls In The Federal Government.

However, the Mission's records showed that it had performed a risk analysis, had contingency plans and had an offsite backup facility in the event of an emergency (see page 8).

Summary of Recommendations

This report contains no recommendations.

Management Comments and Our Evaluation

In its written response to the draft report, management issued a representation letter consistent with the guidance issued by A.I.D./Washington on May 13, 1992 and requested that all disclaimers included in the audit report be deleted. The Mission also requested that the representation letter be included as an annex to the audit report (see Appendix II, pages 23 and 24).

The Director of USAID/Zimbabwe did provide us with limited written assurances, but Mission managers would not confirm in writing, to the best of their knowledge and belief,

the information we deemed essential to answer our audit objectives. A complete analysis of the information that we requested from the Mission Director, Controller and the Systems Administrator to confirm to us in a representation, and the limited written assurance, signed only by the Mission Director, provided in response are found on pages 17 and 18 of this report. The Reports on Internal Controls and Compliance are found on pages 9 and 14, respectively.

Office of the Inspector General

Office of the Inspector General
July 29, 1992

Table of Contents

	Page
EXECUTIVE SUMMARY	i
INTRODUCTION	
Background	1
Audit Objectives	2
REPORT OF AUDIT FINDINGS	4
1. Has USAID/Zimbabwe 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?	5
2. Does the System Administrator maintain physical security measures that safeguard the Wang VS Systems as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government?	6
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?	7
4. Has USAID/Zimbabwe performed a 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?	8
REPORT ON INTERNAL CONTROLS	9
REPORT ON COMPLIANCE	14

MANAGEMENT COMMENTS AND OUR EVALUATION

16

Appendix

SCOPE AND METHODOLOGY

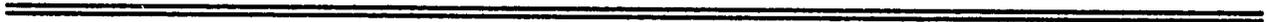
I

MANAGEMENT COMMENTS TO THE DRAFT REPORT

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 the IRM.

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 the Fiscal Year ended September 30, 1990, the USAID/Zimbabwe Controller's Office had obligated about \$130.1 million, committed \$120.0 million, and disbursed \$112.8 million for active agricultural, basic education and manpower development activities in Zimbabwe. A strong 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.

Audit Objectives

As part of a world-wide audit, the Office of the Regional Inspector General for Audit, Nairobi conducted an audit of USAID/Zimbabwe's Security of the Wang VS as related to MACS to answer the following audit objectives:

1. Has USAID/Zimbabwe assigned responsibilities for automation security as suggested
- 11

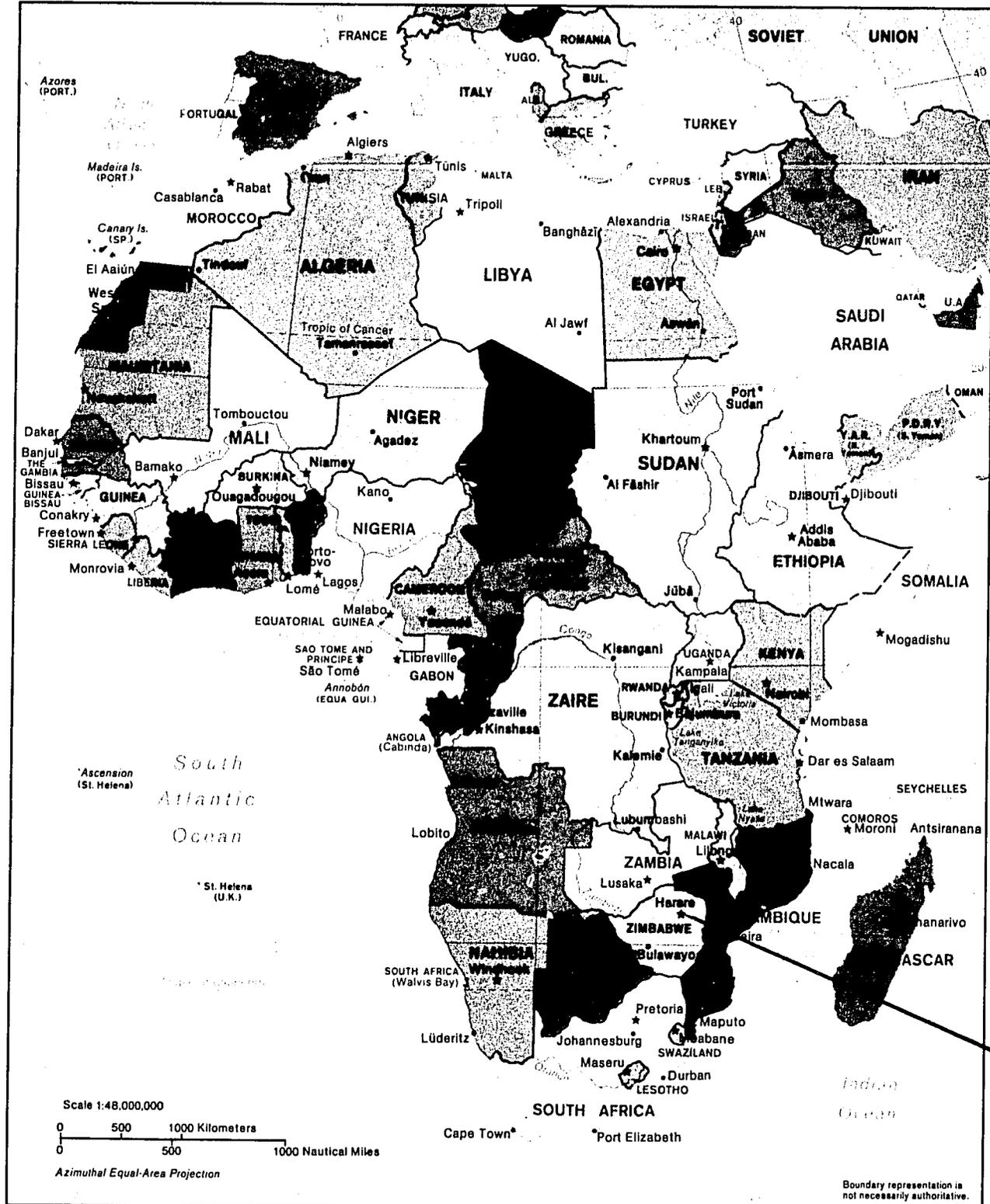
in A.I.D.'s Automation Security Guidebook and required by "specific" Standards For Internal Controls In The Federal Government?

2. Does the System Administrator maintain physical security measures that safeguard the Wang VS Systems 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/Zimbabwe performed a 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?

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 would have been sufficient to provide reasonable--but not absolute--assurance that our answers to the audit objectives would have been valid if management had provided an acceptable representation letter.

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

Africa



REPORT OF AUDIT FINDINGS

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

For example, USAID/Zimbabwe'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/Zimbabwe would not provide or confirm is provided in the Scope and Methodology section of this report.)

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

While we cannot state positively that USAID/Zimbabwe 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. However, based on the information that USAID/Zimbabwe did provide to us and the tests that we were able to perform, no problem came to our attention other than USAID/Zimbabwe's inability to confirm essential information about its own operations.

1. Has USAID/Zimbabwe 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 four, because of the limitations placed on the audit by management, we are unable to fully answer whether USAID/Zimbabwe assigned responsibilities for automation security 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.

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, GAO'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, a USAID/Zimbabwe official stated that the system's security function is assigned to the Executive Officer, an American direct-hire employee. The official also stated that reporting to the executive officer and independent from accounting functions and activities, is the systems manager, who is responsible for overseeing the day-to-day operations of the Wang VS automated system at USAID/Zimbabwe, including security related activities.

2. Does the System Administrator maintain physical security measures that safeguard the Wang VS Systems 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 four, because of the limitations placed on the audit by management, we are unable to fully answer 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.

The Automation Security Guidebook suggests that all automated systems should be kept in a secure and 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/Zimbabwe 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/Zimbabwe's records, the Systems Administrator maintained an inventory system of Wang VS-related equipment by model number, serial number and location. These records also showed that computer hardware and related equipment were accounted for.

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 four, because of the limitations placed on the audit by management, we are unable to fully answer 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.

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 changed or deleted, if appropriate, 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, according to the Systems Administrator, 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.

4. Has USAID/Zimbabwe performed a 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?

As discussed on page four, because of the limitations placed on the audit by management, we are unable to fully answer whether USAID/Zimbabwe performed a 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 the General Accounting Office's (GAO) "specific" Standards For Internal Controls In The Federal Government.

A.I.D.'s Automation Security Guidebook states that risk analysis and contingency planning for automated information resources should be accomplished by each mission. Specifically, contingency plans should address the following:

- back-up of critical hardware, software and data including back-up processing agreements with other agencies or companies having similar facilities;
- specific responsibilities for executing the plan;
- the priority of each activity; and
- procedures for notifying key personnel.

In addition, the 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 Mission provided us with documentation and showed us that it had performed a risk analysis, had a documented contingency plan and had a offsite backup facility available in the event of an emergency.

REPORT ON INTERNAL CONTROLS

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

We have audited USAID/Zimbabwe's internal controls for the Wang VS Security System for the period January 7, 1992 through January 16, 1992, and have issued our report thereon dated July 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/Zimbabwe 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/Zimbabwe 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/Zimbabwe's internal controls relating to assigned responsibilities for automation security and 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/Zimbabwe did provide and tests that we were able to perform, we can report only that no significant internal control weaknesses came to our attention, other than USAID/Zimbabwe'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/Zimbabwe'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/Zimbabwe did provide to us and the tests that we were able to perform, we can report only that no significant internal control weaknesses came to our attention, other than USAID/Zimbabwe's inability to confirm essential information about its own internal controls.

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/Zimbabwe'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/Zimbabwe did provide to us and the tests that we were able to perform, we can report only that no significant internal control weaknesses came to our attention, other than USAID/Zimbabwe's inability to confirm essential information about its own internal controls.

Conclusions for Audit Objective Four

Has USAID/Zimbabwe performed a 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?

We assessed USAID/Zimbabwe'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/Zimbabwe did provide to us and the tests

that we were able to perform, we can report only that no significant internal control weaknesses came to our attention, other than USAID/Zimbabwe's inability to confirm essential information about its own internal controls.

REPORT ON COMPLIANCE

This section summarizes our conclusions on USAID/Zimbabwe's compliance with the Federal Managers' Financial Integrity Act (FMFIA) which requires each mission to comply with the Act as set forth by binding policies in Department of State cables sent to the missions each year.

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/Zimbabwe 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 which requires each mission to comply with the Act as set forth by binding policies in Department of State cables sent to the missions each year.

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/Zimbabwe's compliance with the general assessment cable guidance for 1991. As management was not willing to confirm in a representation letter essential information related to such compliance, we cannot therefore state positively that USAID/Zimbabwe complied. However, based on the information that USAID/Zimbabwe did provide to us and the tests that we were able to perform, we can report that USAID/Zimbabwe performed an internal control assessment (which included the Mission Accounting and Control System) for the year ending September 30, 1991, and that no irregularities or instances of violations of binding policy came to our attention.

MANAGEMENT COMMENTS AND OUR EVALUATION

In its written response to the draft report, management issued a representation letter consistent with the guidance issued by A.I.D./Washington on May 13, 1992 and requested that all disclaimers included in the audit report be deleted. The Mission also requested that the representation letter be included as an annex to the audit report (see pages 23 and 24).

The Director of USAID/Zimbabwe did provide us with limited written assurances, but Mission managers would not confirm in writing, to the best of their knowledge and belief, the information we deemed essential to answer our audit objectives. A complete analysis of the information that we requested from the Mission Director, Controller and the Systems Administrator to confirm to us in a representation, and the limited written assurance, signed only by the Mission Director, provided in response are found on pages 17 and 18 of this report.

SCOPE AND METHODOLOGY

Scope

We performed the audit of USAID/Zimbabwe's Security of the Wang VS as Related to MACS in accordance with generally accepted government auditing standards, except that USAID/Zimbabwe's management would not provide us with a representation letter confirming information essential to fully answer the audit objectives. Management's refusal to make such representations constitutes a limitation to the scope of the audit. The Director of USAID/Zimbabwe did provide us with limited written assurances (see page 23), but Mission managers would not confirm in writing, to the best of their knowledge and belief, the information we deemed essential to answer our audit objectives. Following is an analysis of the information that we requested from the Mission Director, Controller and the Executive Officer to confirm to us in a representation, and the limited written assurances, signed only by the Mission Director, provided in response.

- We requested the aforementioned Mission officials to confirm whether they are responsible for the internal control system, compliance with applicable laws and regulations, and the fairness and accuracy of accounting and management information for the organization under audit. However, the letter provided to us does not acknowledge these responsibilities.
- We requested the Mission officials to confirm whether they had provided us with all the financial and management information associated with the activity under audit, but the letter provided to us does not confirm this information. Instead, it only attests to the fact that the Director asked his staff to make all records available to us.
- We requested the Mission officials to confirm whether they know of any irregularities in the activity under audit. However, the letter provided to us does not address the question.

- We requested Mission officials to confirm whether they know of any material instances where financial or management information have not been properly and accurately recorded and reported. Instead, the letter provided to us only affirms that the director understands from his staff that the records are complete and accurate.
- We requested the Mission officials to confirm whether they are aware of any instances of noncompliance with A.I.D. policies and procedures or violations of laws and regulations. However, the letter provided to us does not address this question.
- We requested the Mission officials to confirm whether they have complied with contractual agreements. However, the letter provided to us does not address this question.
- We requested the Mission officials to confirm whether they know of any events subsequent to the period under audit that could affect the above representations. However, the letter provided to us does not address this question either.

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 confirm their answers to these questions in writing through a representation letter, then we cannot risk giving a positive opinion.

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, 1990 through September 30, 1991, and reviewed procedures in-place at the time of our field work. The audit field work was conducted from January 7, 1992 through January 16, 1992 in Harare, Zimbabwe. In conducting the audit, we obtained and examined records provided by the Mission, and relied on testimonial evidence from officials of USAID/Zimbabwe and considered related prior audits.

Methodology

Although we were not able to fully answer the audit objectives because of the absence of an acceptable representation letter, we designed and followed an audit program which would

have allowed us to fully answer the audit objectives had we received an acceptable representation letter. We also reviewed USAID/Zimbabwe's Internal Control Assessment for 1991 to determine whether the evaluation disclosed any material weaknesses in the Automated Data Processing area. The methodology for each audit objective follows.

Audit Objective One

Has USAID/Zimbabwe 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 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 reflected ongoing 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 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 discussed 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;
- 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;
- evaluated and tested the procedures for security processing of terminated personnel; and
- reviewed 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" Standard: For Internal Controls In The Federal Government?

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 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 on the computer room door and the security system in place to allow access to the Mission's premises.

We selected a judgmental sample of 7 items out of 174 items from the Mission's inventory listing of Wang VS-related equipment and traced items in the sample by location, model numbers and serial numbers. We selected a judgmental sample because we determined that it was appropriate since the items in the universe were not uniform in terms of dollar amounts, types of items and levels of vulnerability.

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 inquired whether an alarm system had been installed to alert for unauthorized entry to the computer facility; and whether the alarm is engaged to alert the authorities.

We examined logs to verify 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 "specific" Standards For Internal Controls In The Federal Government?

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 asked if there was a dial-up system in use.

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

- reviewing procedures for changing the password when an employee resigns or is terminated;
- reviewing procedures for 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 interviewed the Controller and the Budget and Fiscal Officer who stated that adequate controls exist over rejected transactions, and that rejected transactions are corrected and put back into the system.

Audit Objective Four

Has USAID/Zimbabwe performed a 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?

We reviewed documentation to determine if a risk assessment had been performed on the vulnerability of the Wang VS System.

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



**UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT
MISSION TO ZIMBABWE**

INTERNATIONAL MAIL
1 Paines Avenue
P.O. Box 9918
Harare, Zimbabwe



UNITED STATES MAIL
Agency for International Development
Harare (ID)
Washington DC 20511-2100
U.S.A.

REPRESENTATION LETTER

July 13, 1992

Mr. J. Farinella
RIG/A/Nairobi
Union Towers Building
Moi Ave/Mama Ngina St
Nairobi
Kenya

Dear Mr. Farinella:

This is in regard to the audit which you have recently completed on USAID/Zimbabwe's security of the Wang VS as related to MACS. I have asked appropriate members of my staff to make available to you all records in our possession for the purpose of this audit. Based on the representations made by those individuals to me, I believe that those records are accurate and complete, and that they give a fair representation as to the status of USAID/Zimbabwe's security of the Wang VS as related to MACS. After review of your draft audit report and consultation with my staff, I know of no other facts (other than those expressed in the Mission comments given in response to the draft report) which, to the best of my knowledge and belief, would materially alter the conclusions reached in the draft report.

I request that this Representation Letter be considered a part of the official Mission comments on the draft report, and be published along therewith as an annex to the report.

Sincerely,

Ted D. Morse
Mission Director

Phone 726630/720799-720757
Country Code 263, City Code 4
Telex No. 24425 ZW
Fax No. 722418

UNITED STATES GOVERNMENT

memorandum

DATE: July 13, 1992

REPLY TO
ATTN OF: Ted D. Morse, Director, USAID/Zimbabwe *DM*

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

TO: Joseph Farinella, RIG/A/Naircbi

Ref: Memorandum dated January 31, 1992 Spielman/Farinella

Enclosed is the Mission's Representation Letter on the subject audit. This letter is issued consistent with the latest guidance we have received from AID/W (guidance is dated May 13, 1992) on audit representation letters. Given our response is consistent with AID/W guidance, it is our opinion that all disclaimers included in the audit report should be deleted.

I understand that you have spoken with Ms. Lewellen, our Controller and advised her that the IG has not accepted the Agency guidance. Nevertheless, I believe, that in good faith, the report must now indicate that the Mission issued an audit representation letter which was consistent with the Agency guidance, but the IG has not accepted such.

Our comments on the draft report remain unchanged.

OPTIONAL FORM NO. 10
(REV. 1-80)
GSA FPMR (41 CFR) 101-11.6
5010-106

APPENDIX III

Report Distribution

American Ambassador to Zimbabwe	1
Administrator (A/AID)	2
Mission Director, USAID/Zimbabwe	5
AA/AFR	1
AFR/SA/ZZMS	1
AFR/CONT	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
FAMCS	2
FA/FM/FPS	2
REDSO/ESA	1
REDSO/RFMC	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