
**AUDIT OF USAID/PAKISTAN'S SECURITY
CONTROLS FOR THE WANG VS COMPUTER
USED TO SAFEGUARD THE MISSION
ACCOUNTING AND CONTROL SYSTEM (MACS)**

**Audit Report No. 5-391-92-06
June 30, 1992**





U.S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

June 30, 1992

MEMORANDUM

TO: Nancy M. Tumavick, Acting Mission Director,
USAID/Pakistan

FROM: *James B. Durnil*
James B. Durnil, RIG/A/Singapore

SUBJECT: Audit of USAID/Pakistan's Security Controls for the Wang VS Computer Used to Safeguard the Mission Accounting and Control System (MACS), Audit Report No. 5-391-92-06

Enclosed are five copies of our audit report on USAID/Pakistan's Security Controls for the Wang VS Computer Used to Safeguard the Mission Accounting and Control System (MACS). In the preparation of this report, we considered your comments to our draft report and also included your comments in total as Appendix II to this report.

Based on our audit work and the written representations provided by USAID/Pakistan officials, we can positively report that an adequate system of internal controls was established by USAID/Pakistan to safeguard its Wang VS computer system. Further, except for the three problem areas discussed in this report, we can report that USAID/Pakistan complied with the guidance of the A.I.D. Automation Security Guidebook and the requirements set forth in the Standards for Internal Controls in the Federal Government. USAID/Pakistan has established good security controls for MACS.

This report contains three recommendations. Recommendations Nos. 2.1 and 2.2 are resolved and will be closed upon the issuance of this report. Recommendation Nos. 1 and 3 will be resolved when agreement is reached between the Mission and us on how to implement the recommendations. The recommendations will be closed when USAID/Pakistan provides us with: (1) documentation that the recommended procedures have been established and implemented; or (2) documentation of a cost/benefit analysis and the implementation of the actions, if any, that logically flow from the review.

Please provide us information within 30 days indicating any actions planned or taken to implement the open recommendations. I appreciate the cooperation and courtesies extended to my staff during the audit.

Attachments: a/s

EXECUTIVE SUMMARY

USAID/Pakistan operates a Wang VS computer system which is used to process the Mission's information resources. One of the primary programs operating on this system is the Mission Accounting and Control System (MACS). MACS is used by the Office of Financial Management as the automated financial management system for the Mission. Since A.I.D. recognizes its information resources to be very valuable assets, they have prepared an Automation Security Guidebook to set forth Agency policies and procedures for safeguarding these resources.

We audited USAID/Pakistan's security controls of the Wang VS computer used to safeguard the Mission Accounting and Control System. The audit was conducted in accordance with generally accepted government auditing standards and covered procedures in place at the time of our field work from December 2, 1991 through December 17, 1991.

USAID/Pakistan designated the Executive Officer to be the Systems Security Officer (page 4) who directs the implementation of the computer security policies described in the A.I.D. Automation Security Guidebook.

USAID/Pakistan's physical security controls, designed to protect their Wang VS system, are consistent with the policies described in the A.I.D. Automation Security Guidebook (page 6). USAID/Pakistan also satisfied the Access and Accountability for Resources "specific" Standard for Internal Controls in the federal government, by limiting access to the computer room to authorized individuals.

USAID/Pakistan's System Administrator is 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 (page 8) except:

- Passwords stored on the Mission's Wang VS system are not encrypted (page 9). Therefore, system managers and other knowledgeable users

can exploit the rights and privileges that are assigned exclusively to financial officers; and

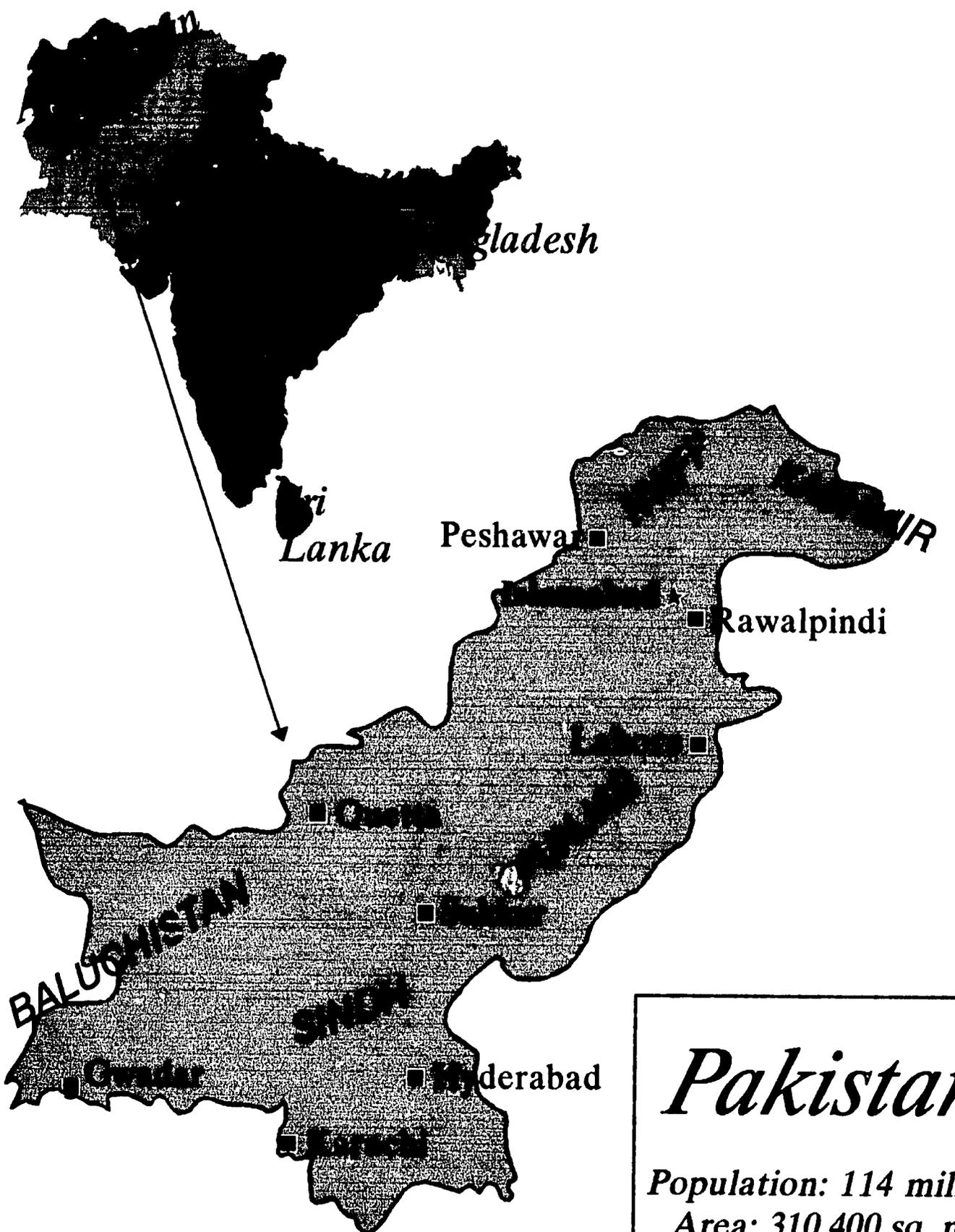
- The System Administrator does not maintain a log of transactions performed with the system's security software (page 12). Because this security information is otherwise not readily available, the Systems Security Officer cannot easily review the work of the system managers and identify possible security violations. Unauthorized access to the Wang VS system may thus go undetected.

USAID/Pakistan officials performed risk analyses and developed a contingency plan for their automated information resources but their plan does not include written procedures that can be immediately followed in the event of a system disaster (page 15). Without such explicit instructions, the contingency plan is incomplete and ineffective.

This report contains three recommendations, and also presents our assessment of internal controls (page 18) and compliance with laws and regulations (page 23).

In responding to the draft report, USAID/Pakistan agreed to maintain and review computer security logs but did not think that the controls of: (1) encrypted passwords and (2) a detailed contingency plan containing step-by-step instruction, could be justified because the implementation costs would exceed the benefits gained. USAID/Pakistan's comments are summarized after each finding and included in total as Appendix II of this report.

Office of the Inspector General
Office of the Inspector General
June 30, 1992



Pakistan

Population: 114 million

Area: 310,400 sq. mi.

Capital: Islamabad

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	i
INTRODUCTION	1
Background	
Audit Objectives	1
REPORT OF AUDIT FINDINGS	
Audit Objective One — Has USAID/Pakistan assigned the responsibilities for automation security as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the federal government?	4
Audit Objective Two — 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?	6
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?	8
Passwords Stored on the Mission's Wang VS System Are Not Encrypted.	9
Security Logs Are Not Maintained and Reviewed.	12
Audit Objective Four — Has Mission Management performed risk analysis and developed an adequate contingency plan for their automated information resources as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the federal government?	15
USAID/Pakistan's Contingency Plan Does Not Include Action Steps.	15

TABLE OF CONTENTS

REPORT ON INTERNAL CONTROLS	18
REPORT ON COMPLIANCE	23
APPENDICES	<u>Appendix</u>
SCOPE AND METHODOLOGY	I
MANAGEMENT COMMENTS	II
REPORT DISTRIBUTION	III

INTRODUCTION

Background

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

USAID/Pakistan's Wang VS system is operated by the Automatic Data Processing Division, which is organized within the Office of Management. The MACS system is used by the Office of Financial Management to record accounting transactions. USAID/Pakistan obligated/deobligated a net deobligation of \$47,714,000, committed \$169,814,000, and disbursed \$181,332,000 during fiscal year 1991. Because of this large dollar volume, strong computer security controls are necessary to ensure that: the use of resources is consistent with laws, regulations, and policies; resources are safeguarded against waste, fraud, and misuse; and reliable data are obtained, maintained, and fairly disclosed in reports.

Audit Objectives

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

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

Does 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?

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?

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

Our review was made in accordance with generally accepted government auditing standards and included such tests of 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 problem, and

- **make recommendations to correct the condition and cause of the problem.**

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

REPORT OF AUDIT FINDINGS

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

USAID/Pakistan assigned the responsibilities for automation security as suggested in A.I.D.'s Automation Security Guidebook and required by "specific" Standards for Internal Controls in the federal government.

USAID/Pakistan designated the Executive Officer as the Systems Security Officer (SSO) for managing and implementing the automated information system security program. This follows the policy prescribed by A.I.D.'s Automation Security Guidebook that each overseas mission with an automated information system designate an American employee to be the Systems Security Officer. USAID/Pakistan's Wang VS system is operated by their Automatic Data Processing Division, which, as part of the Office of Management, reports directly to the Executive Officer. The Automatic Data Processing Division consists of a staff of six employees. The Systems Specialist (System Manager) serves as chief of this branch and has the primary responsibility for supervising and managing the Mission's entire computer operations. He is supported in this task by the Systems Analyst, who acts as his deputy. These two individuals perform the day-to-day security functions associated with the Wang VS system including: adding and deleting users, changing users' access privileges, assigning passwords, and making backup copies of computer files.

Since the Executive Officer reports directly to the Mission and Deputy Mission Directors, assigning computer security responsibilities to him, places the Systems Security Officer high enough in the Mission's organization to allow him to act independently. His position within the organization also separates the responsibility for controlling the access to computer resources from the responsibilities for recording accounting transactions and certifying payments

which are performed by the Office of Financial Management. Therefore, this organizational structure complies with the separation of duties "specific" Standard for Internal Controls in the federal government.

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 the "specific" Standards for Internal Controls in the federal government?

The System Administrator maintains physical security measures that safeguard the Wang VS system as suggested in A.I.D.'s Automation Security Guidebook and required by the "specific" Standards for Internal Controls in the federal government.

USAID/Pakistan's physical security controls, designed to protect their Wang VS system, are consistent with the policies described in the A.I.D. Automation Security Guidebook. USAID/Pakistan also satisfied the Access and Accountability for Resources "specific" Standard for Internal Controls in the federal government, by limiting access to the computer room to authorized individuals.

The central unit of USAID/Pakistan's Wang VS system is a Wang VS100 minicomputer with six disk drives and one tape drive which are all located within their computer room. The auditors observed the following controls protecting this equipment:

- limited access (one door secured with a lock);
- no ground level windows;
- a location apart from possible hazards such as water pipes;
- a smoke detector installed inside the room;
- a hand-held fire extinguisher located in the room;
- a master power shut-off switch; and
- clean electric power provided by an uninterrupted power supply (UPS) equipment.

Additional security controls are in place because the computer room is located within USAID/Pakistan's secured office building. The building is protected by guards on duty 24 hours a day. Employees are issued identification cards and visitors must obtain passes from the receptionist prior to being admitted to the office area.

Since USAID/Thailand's physical security controls follow the guidance of the A.I.D. Automation Security Guidebook and also satisfy the "specific" Standards for Internal Controls in the federal government, the risk of physical damage to computer resources has been reduced to an acceptable level.

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?

USAID/Pakistan's System Administrator is 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, except: passwords stored on the Mission's Wang VS system are not encrypted; and security logs are not maintained and reviewed.

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

The Systems Manager and his deputy create user identifications and passwords with the Wang VS security software. This identification data is stored on the system in a users list file, which the system employs to authenticate users when they log on. This control reduces the risk of non-authorized individuals accessing the Wang VS system.

Once the system validates a user's identification and password, it will determine whether the user has a log-on procedure. This procedure is a series of codes processed automatically by the system, which is specific to a user and which results in a menu allowing access to certain programs. For example, only the staff the Office of Financial Management are assigned menus that allow them to access the accounting programs. This control prevents unauthorized users from viewing or manipulating sensitive accounting data. All USAID/Pakistan employees except for the two system administrators have specified log-on procedures, allowing access to only those programs included on their menus.

Each file on the system may be assigned to one (and only one) specified file protection class, which is indicated by a one-character file class code. The System Administrator may establish up to 26 file classes, and assign files to each class in a logical manner. Users are subsequently allowed or denied access to file classes, and allowed or denied modes of access (read, execute, or write). For example, USAID/Pakistan's Systems Manager has assigned financial files in the MACS and

MACSTRAX accounting systems to file classes only accessible to the staff of the Office of Financial Management. This prevents unauthorized users from accidentally or maliciously altering accounting records.

Even though USAID/Pakistan is effectively using the Wang VS security software to reduce the risk of accounting information being lost or altered, the risk could be further reduced if passwords were encrypted and computer log files were maintained and reviewed. These two problem areas are discussed in detail below.

Passwords Stored on the Mission's Wang VS System Are Not Encrypted

Users' passwords to the Mission's Wang VS system are stored on the system in a file that is in a readable format, even though encrypting passwords is identified as a common-sense security measure in the A.I.D. Automation Security Guidebook. "Encrypting" a password entails scrambling it in such a way that it cannot be read by any user, regardless of their level of access to the system. Because the A.I.D. Automation Security Guidebook does not contain specific information on password encryption for the Wang VS computer, USAID/Pakistan did not consider purchasing optional software that would make this encryption possible. As a result, system managers and other knowledgeable users may be able to access the files where passwords are stored and learn the passwords for all system users. With these passwords, they can log onto the system as other users, and then access confidential data reserved exclusively for financial officers or other key personnel.

Recommendation No. 1: We recommend that USAID/Pakistan improve computer security by encrypting the passwords stored on their Wang VS system. They should purchase the software upgrades necessary for encrypting passwords and enabling users to change their own passwords.

Users' passwords to the Mission's Wang VS system are stored on the system in a file that is in a readable format. Any user who can access this file can learn the identifications and passwords for all system users—even users with special privileges such as financial officers, accountants, and voucher examiners.

Because of the sensitivity of accounting data, the staff of the Office of Financial Management should have exclusive access to the two financial software packages

located on USAID/Pakistan's Wang VS computer: MACS and MACSTRAX. MACS (Mission Accounting and Control System) is a processing system in which accounting transactions are recorded in ledgers and other control files. MACSTRAX (Mission Accounting and Control System Voucher Tracking System) is an automated voucher management system used to record, track, verify, and schedule payments. Since MACS and MACSTRAX contain sensitive financial data and provide the ability to manipulate this data, it is imperative that USAID/Pakistan protect these systems with strong security controls.

The A.I.D. Automation Guidebook considers encrypting passwords a common-sense security measure, because files containing password data are among the most sensitive in the entire system. Although these files are subject to access controls, knowledgeable individuals may be able to bypass the controls. Encrypting the files containing passwords secures them from unauthorized reading or modification, while they are still available for checking when logging onto the system. Passwords should be one-way encrypted so that they cannot be subsequently decrypted. In this way, when a user logs onto the system, the password that he/she types on the keyboard is immediately encrypted and compared with that user's password stored in the encrypted password file.

A division of responsibilities over the assignment of passwords is desirable. The System Administrator assigns a user ID and the initial password for each user. The first time the user logs on with this ID and password, the system will require the user to select a new password which will not be known to the System Administrator. Since this user-defined password is stored on the system in an encrypted format, the System Administrator cannot log on with another user's ID without changing that user's password. If this should happen, however, that user will be aware that his/her password has been changed the next time he or she attempts to log onto the system, and can immediately report the matter.

The Wang security software being used by USAID/Pakistan (Wang VS Operating System version 7.20) can, optionally, be enhanced to provide encrypted passwords and users' ability to change their own passwords. Since the Mission has not purchased this option, they are unable to encrypt their password files.

The A.I.D. Automation Security Guidebook does not provide specific guidance on password encryption for the Wang VS system. It suggests that the Systems Security Officer encrypt or otherwise protect from unauthorized access the computer-stored password file but it fails to define "otherwise protect". It also does not address the password encryption capability of the Wang VS computers and does not identify the optional software necessary for encrypting passwords.

Without specific guidance, USAID/Pakistan did not assess the risk of non-encrypted passwords and measure this risk against the cost of upgrading their security software. Although the design of the Automation Security Guidebook is beyond the scope of our audit objectives, its lack of guidance on password encryption contributed to this problem area. A separate audit is planned in Washington which will address the effectiveness of the guidebook and make recommendations for correcting any identified weaknesses.

Without the security control of encrypted passwords, the risk of an unauthorized individual logging onto the Wang VS system without detection is unnecessarily high. This risk may be acceptable for non-critical computer resources, but since financial officers have powerful capabilities and privileges through the MACS and MACSTRAX application programs, strong controls are necessary to protect their access rights.

Management Comments and Our Evaluation

USAID/Pakistan stated that there wasn't a single user at the Mission, except the system administrators, who could read the Wang VS user list containing user IDs and passwords; "even knowledgeable individuals familiar with the VS operating system cannot bypass this control". Therefore they contend that any benefits obtained from a password encryption program would not justify the five to six thousand dollars such a program would cost.

Password encryption is not an extreme security procedure. It is the corner stone of any commercial computer security software sold for computers ranging from the largest main frames to office networks and stand-alone microcomputers. This may well be why the A.I.D. Automation Guidebook lists encrypting passwords under common-sense security measures.

We agree that the implementation of any control should be evaluated considering its cost in relation to its benefits. Therefore, USAID/Pakistan's decision should be based on a thorough analysis which includes technical input from the AID/Washington computer staff. Once USAID/Pakistan has completed their analysis, they should provide us with the documentation of their review and their resulting decisions.

Security Logs Are Not Maintained and Reviewed

USAID/Pakistan's System Administrator does not maintain a log of all transactions performed with the security software of the Wang VS system. Although A.I.D.'s Automation Security Guidebook does not comment on maintaining security logs, the GAO "specific" internal control standards require: (1) that transactions be documented and (2) that qualified personnel continuously supervise the work of subordinates. Security logs furnish both the documentation and, when reviewed regularly, an important supervision tool for non-technical managers. Because of lack of guidance in the A.I.D. Automation Security Guidebook, the Systems Security Officer was not aware of the importance of maintaining and reviewing computer security logs. Without security logs, USAID/Pakistan's management is unable to easily review the work of the system managers and identify possible security violations. Unauthorized access to the Wang VS system may thus go undetected.

Recommendation No. 2: We recommend that USAID/Pakistan:

- 2.1 Use the security software of the Wang VS system to log: (a) all transactions performed with the security software of the Wang VS system; (b) all files that are restored to the system; and (c) all attempted log-ons with invalid or mismatched user identifications or passwords.**
- 2.2 Implement procedures requiring the Systems Security Officer to review computer security logs on a daily or weekly basis.**

The System Administrator does not maintain a log of security transactions performed on the Wang VS system. Therefore, security transactions are not documented and cannot be reviewed by his supervisor. The Systems Security Officer's only mechanism for identifying security violations is relying on the System Administrator to bring them to his attention.

Using the Wang security software, the System Administrator and his deputy perform such security transactions as adding and deleting users, changing users' access privileges, and assigning passwords. In addition, the Wang security software is used to establish both log-on procedures and specific access rights to file classes for each user. Through these two security controls (discussed above),

users' access to software applications and data is controlled. For example, only the Office of Financial Management staff and users with system administrator privileges have the ability to modify MACS data files.

Common-sense computer security procedures dictate that all changes to the security files, including those involving user identifications, passwords, user privileges, and access rights, should be logged. This documentation of transactions is also required by the "specific" Standards for Internal Controls in the federal government. The log should indicate the identity of the person making the change, the type of change, and the people whose authorizations are being changed.

A security system must also be able to identify all attempted violations, whether accidental or malicious. Any mismatch of user ID and password or any unauthorized request to access data should be recorded in a log. The Systems Security Officer's regular review of the security violation log may identify unusual activity. Once unusual activity is detected, it can be followed up on to determine if someone is attempting unauthorized access to the system. Also, a data file owner should be notified of all unauthorized attempts to read or change records in his or her files.

In addition to basic computer security needs, log files provide non-technical managers with a tool for supervising the work of technical computer personnel. The "specific" Standards for Internal Controls in the federal government require supervisors to continuously review and approve the assigned work of their staffs. Computer security logs document the work of the technical staff (system administrators). By regularly reviewing these logs, the Systems Security Officer is able to provide the required supervision.

The A.I.D. Automation Security Guidebook does not require computer security logs to be maintained and does not provide specific guidance on the capability of the Wang VS software for producing security logs. Without this specific guidance, the Systems Security Officer was not aware of the importance of maintaining computer security logs. Although the design of the Automation Security Guidebook is beyond the scope of our audit objectives, its lack of guidance on maintaining and reviewing security logs contributed to this problem area. A separate audit is planned in Washington which will address the effectiveness of the guidebook and make recommendations for correcting any identified weaknesses.

Version 7.20 of the Wang VS operating system, which is used by USAID/Pakistan, provides event-logging tools which allow system administrators to create, maintain, and protect an audit trail on specified events such as file access and user log-ons. By not taking advantage of these capabilities, the Systems Security Officer cannot adequately supervise the computer staff and cannot easily identify possible security violations. Unauthorized access to the Wang VS system may thus go undetected.

Management Comments and Our Evaluation

USAID/Pakistan stated that they have implemented Recommendation Nos. 2.1 and 2.2 on April 15, 1992. Therefore, this recommendation will be considered closed upon the issuance of this report.

USAID/Pakistan should also discuss their implementation of this recommendation with the AID/Washington computer staff. The AID/Washington staff may be able to provide some suggestions that will counter the effect computer logs are having on computer capacity and performance. In addition, AID/Washington may be able to use USAID/Pakistan's experience to benefit other missions.

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

Mission Management has performed 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 except USAID/Pakistan's contingency plan does not include action steps.

USAID/Pakistan has performed an analysis of the risk of losing their automated information resources. Their analysis identified likely threats that might disrupt or destroy their computer operations, and determined the intrinsic value associated with key systems that rely on the Mission's computers. They have also implemented controls to ensure a rapid recovery from any disruption of these systems. For example, USAID/Pakistan has designed, documented, and implemented a system for producing back-up copies of key data files on a daily basis and system files on a weekly basis. These back-up tapes are not stored at USAID/Pakistan's building but at the American Embassy, Islamabad and at USAID/Pakistan's warehouse. This off-site storage reduces the chances of the original computer data and back-up data being damaged by the same disaster.

USAID/Pakistan has a written agreement with the American Embassy, Islamabad for providing emergency use of their Wang VS system in the event that USAID/Pakistan's system is not operable for a short period of time. A.I.D./Cairo will be used as the processing center for the MACS and MACSTRAX application if USAID/Pakistan's facilities are unavailable for a prolonged period.

Although USAID/Pakistan has identified likely threats to their computer operations and implemented procedures for backing up computer files, they did not prepare explicit instructions that guarantee a complete and effective response to a disaster.

**USAID/Pakistan's Contingency Plan
Does Not Include Action Steps**

USAID/Pakistan's contingency plan for their computer resources does not include written procedures that can be immediately followed in the event of a system disaster. This resulted from USAID/Pakistan's failure to fully follow the guidance

in A.I.D.'s Automation Security Guidebook. In an emergency, valuable time may be lost waiting for instructions, and computer resources may be needlessly destroyed.

Recommendation No. 3: We recommend that USAID/Pakistan modify their written contingency plan to include step-by-step instructions for restoring computer operations for each type of disaster identified in their risk assessment.

Immediate response to a disaster may well save valuable computer resources and therefore reduce the time necessary to resume full operations. The A.I.D. Automation Security Guidebook states that a contingency plan should address various levels of threats to their computer operations and specify the actions to be taken in each case. USAID/Pakistan's contingency plan does identify likely threats but it does not include the instructions necessary for a quick response. Without such explicit instructions, the contingency plan is incomplete and ineffective.

Written instructions greatly facilitate rapid recovery from either a short interruption or a catastrophe. Otherwise, the response to an emergency situation is left to chance. The System Administrator, or other persons in charge of computer operations, may not remember the details of a complex recovery system or may not be available. Under such circumstances, the vague ideas of a few people cannot constitute a viable recovery plan.

The Mission should produce a recovery manual providing step-by-step plans defining the responsibilities of each organizational unit. How a mission reacts and the speed at which it reacts when one of these contingencies arises is important. The right decisions can minimize the impact of the disaster, or even prevent the disaster from happening.

The Systems Security Officer was aware of the guidance provided by the A.I.D. Automation Guidebook, and indeed identified his critical ADP systems as well as likely threats to their operations. But he did not complete the process by preparing written procedures that could be immediately followed in the event of a system disaster. Although the A.I.D. Automation Security Guidebook requires contingency plans to specify the actions to be taken for each identified threat, it does not give the detailed guidance a non-technical manager requires to implement this procedure. Computer operations vary but many of the likely threats to computer operations are similar. Therefore, many prevention and recovery actions would also be similar. The Guidebook does not provide the framework for an

effective contingency plan: it does not furnish a standard format, identify common threats, or recommend specific actions to be taken for each identified threat. Without this specific guidance, contingency plans will not be consistent from site to site and the quality and effectiveness of plans will greatly vary. Although the design of the Automation Security Guidebook is beyond the scope of our audit objectives, its lack of guidance on the preparation of a contingency plan contributed to this problem area. A separate audit is planned in Washington which will address the effectiveness of the guidebook and make recommendations for correcting any identified weaknesses.

By not having a written action plan, the Mission is accepting a higher risk than is necessary that computer operations will be disrupted and computer resources lost.

Management Comments and Our Evaluation

USAID/Pakistan does not believe that step-by-step instructions for restoring computer operations for each likely threat is necessary.

"Restoring computer operations after a disaster depends on two factors; 1) a complete backup of the information on the system before the disaster; and 2) a competent staff that would implement the recovery procedure. The specific recovery procedures required for each specific type of disaster requires numerous variables, i.e. the type of disaster, extent of the damage to the computer center, the conditions of each component of the VS-100 system, the availability of funds to procure alternate processing sites and/or personnel, etc."

We agree with USAID/Pakistan to the extent that backup copies of computer files and competent personnel are tremendous assets for recovering from a disaster. But it is also true that a written step-by-step contingency plan—prepared by competent personnel—helps insure effective recovery actions will be promptly implemented regardless of the availability of key personnel. This is especially applicable in the foreign service environment where staff is often rotated and travel away from post is routine.

Since our recommendation is in accordance with the criteria contained in the A.I.D. Automation Security Guidebook, USAID/Pakistan should seek assistance from the AID/Washington computer staff. The AID/Washington staff may be able to expound upon the general instructions contained in the guidebook. They may also be able to provide examples of disaster contingency plans applicable to A.I.D.'s overseas missions.

REPORT ON INTERNAL CONTROLS

We have audited USAID/Pakistan's internal controls for the Wang VS computer used to safeguard the Mission Accounting and Control System (MACS) that were in place at the time of our field work from December 2, 1991 through December 17, 1991, and have issued our report thereon dated June 30, 1992.

Scope of Our Internal Control Assessment

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

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

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

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

General Background on Internal Controls

Under the Federal Managers' Financial Integrity Act and the Office of Management and Budget's implementing policies, A.I.D.'s management is responsible for establishing and maintaining adequate internal controls. The 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 are to provide management with reasonable—but not absolute—assurance that: resource use is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data is obtained, maintained, and fairly disclosed in reports.

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

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

Explanation of Categories Evaluated

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

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

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

custody and use of resources is to be assigned and maintained. Periodic comparison of the resources shall be made with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

Conclusions for Audit Objective 1

Has USAID/Pakistan identified and 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 objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the federal government. Our conclusions are summarized below.

We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective. Our tests showed that the internal controls were logically and consistently applied.

Conclusions for Audit Objective 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?

To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the federal government. Our conclusions are summarized below.

We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective. Our tests showed that the internal controls were logically and consistently applied.

Conclusions for Audit Objective 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?

To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the federal government. Our conclusions are summarized below.

We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective. Our tests showed that the internal controls were logically designed and consistently applied except for the following weakness.

- The System Administrator was not maintaining a log of security transactions performed on the Wang VS system, and was therefore not clearly documenting transactions and significant events. With no transaction logs available for review, continuous supervision of the Information Systems Manager and Operations Assistant is difficult.

Conclusions for Audit Objective 4

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

To answer this objective we assessed the design and operation of the controls in place to address the six "specific" Standards for Internal Controls in the federal government. Our conclusions are summarized below.

We reviewed the controls for documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources related to this objective. Our tests showed that the internal controls were logically designed and consistently applied except for the following weakness.

- the contingency plan for computer resources does not include written steps that can be immediately followed in the event of a system disaster. Therefore, the controls in place do not satisfy the documentation standard.

Reporting Under Federal Managers' Financial Integrity Act

USAID/Pakistan's Internal Control Assessments for 1989 identified password protection as a possible security weakness because at that time, user IDs were shared among several people but otherwise did not address the internal weakness identified in this report. In 1990, an abbreviated Internal Control Assessment was prepared which did not comment on computer security. To improve reporting under the Federal Managers' Financial Integrity Act, USAID/Pakistan should perform an assessment of the internal control weaknesses identified in this report and report any unresolved weaknesses in their next report.

REPORT ON COMPLIANCE

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

Scope of Compliance Assessment

We conducted our audit in accordance with generally accepted government auditing standards which require that we:

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

General Background on Compliance

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

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

Conclusions on Compliance

We found no instances of noncompliance with applicable laws and regulations except for the situations of noncompliance with the Standards For Internal Controls In The Federal Government which we addressed in our report on internal controls (see page 18).

SCOPE AND METHODOLOGY

Scope

We audited USAID/Pakistan's security controls of the Wang VS system as related to MACS. We conducted the audit in accordance with generally accepted government auditing standards for performance audits. The audit covered security applications and procedures in place during the audit field work from December 2, 1991 through December 17, 1991.

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

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

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

Methodology

The methodology for each audit objective follows.

- 25''

Audit Objective One

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

To accomplish this audit objective, we prepared an organizational chart identifying operational responsibilities for security controls for the technical and physical security of the Mission's hardware and software. We discussed the chart with security officials to ensure that it accurately reflected ongoing security control practices. We also identified the relevant security controls in place and determined whether they followed the guidance of the A.I.D. Automation Security Guidebook and the "specific" Standards for Internal Controls in the federal government.

Next, we reviewed policy statements and related communications from top management officials that supported the independence of the information system functions. We determined whether the Security Officer provides system security training as well as periodic security briefings to all persons with access to the automated systems.

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

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

Audit Objective Two

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?

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

We also examined how easily one could access the computer room. In this regard, we observed the type of locking equipment, the badge system allowing access, and whether

26

unauthorized individuals were challenged when entering the proximity of the computer area.

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

Audit Objective Three

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?

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

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

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

Audit Objective Four

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

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

- Identified likely threats;

21

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

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

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

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



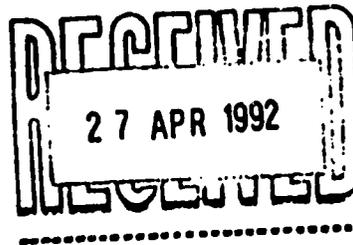
UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT
MISSION TO PAKISTAN

18 - Sixth Avenue, Ramna 5, Islamabad
Post Office Box 1028

Fax : 92-51-824086
Telex : 82-5427 PK
Telephone : 824071-79

THE DIRECTOR

Mr. James Durnil
RIG/A/Singapore
#17-03 Peninsula Plaza
111, North Bridge Road
Singapore 0617



April 22, 1992

Subject: Draft Report on the Audit of USAID/Pakistan's Security Controls For The Wang VS Computer As They Relate to MACS

Dear Jim:

We have reviewed the subject report and provide you our comments on the attached document. Based upon the comments, I am of the view that all the recommendations may be considered for closure at the time of final report issuance. I also understand from the outcome of your discussion with Linda Martin that subject report will be revised as and where appropriate, especially the contents relating to Representation Letter.

I do appreciate including positive remarks for Audit Objectives 1 and 2 relating to Report On Internal Controls which read Quote However, based on information that USAID/Pakistan did provide and the tests that we were able to perform, we can report that no significant internal control weaknesses came to our attention Unquote. I have also noted with appreciation the concluding positive remarks on Report On Compliance which read Quote However, based on information that USAID/Pakistan did provide to us and the tests that we were able to perform, we can report that no irregularities or instances of violations of such applicable laws and regulations came to our attention. Unquote.

Sincerely


James A. Norris
Director

Attachment: As stated

29

MANAGEMENT COMMENTS

RECOMMENDATION 1.1 - PERFORM A COST BENEFIT ANALYSIS ON UPGRADING THE WANG VS SYSTEM SECURITY SOFTWARE TO A PROGRAM THAT PROVIDES PASSWORD ENCRYPTION, AND ENABLES USERS TO CHANGE THEIR OWN PASSWORDS; AND, IF JUSTIFIED, PROCURE THE SECURITY SOFTWARE UPGRADE.

The Wang VS user list which contains the logon id, access rights, logon procedure and password of all valid users for the VS-100 system, although in a readable format, cannot be read by any user. Contrary to the statement in this report, even knowledgeable individuals familiar with the VS operating system cannot bypass this control. The VS user list file is protected by the VS security program and provides access only to the user defined as Systems Administrator.

The Mission is aware of the sensitivity of the MACS and MACSTRAX application software and has provided exclusive access to these systems to the Office of Financial Management (OFM). Only the OFM staff are provided read/write access to MACS files. MACS has a file of valid user identification that controls access to the system. MACSTRAX has an equivalent file that controls the function allowed for each user which is in the encrypted format. The Mission has recently revised the protection class for these two files which allows exclusive access only to the Mission Controller and Deputy Controller. As an additional security precaution, we have restricted the logon ids of all certifying officers to their respective workstations. Logon procedures restrict the access of the accountants to the MACS system and the vouchers examiners to the MACSTRAX system.

The Mission acknowledges that the Systems Administrator could in fact bypass all the security controls of the MACS and MACSTRAX systems. However, the recommended password encryption program would not prevent a knowledgeable System Administrator from bypassing these controls. Therefore, we believe that encryption of user passwords which prevent the Systems Administrator from knowing these passwords would only promote a misconception that these systems are foolproof and totally secure.

The additional benefits of the password encryption program, i.e. allowing the user to change his/her own password and automatic expiration of passwords does not justify the cost of the program. The Mission's limited OE budget precludes us from spending five to six thousand dollars for this software upgrade when it can be easily bypassed. It is, therefore, the Mission's position that based on the cost benefit analysis, the investment of several thousand dollars does not justify the software upgrade.

The Mission agrees that implementation of the report's recommendation 2.1 and 2.2 would improve security controls of the MACS and MACSTRAX and provide the Systems Security Officer a mechanism to supervise systems security on the VS 100. The

enhancement in recommendations 2.1 and 2.2 would provide the necessary security up-grade to meet the recommended standards.

RECOMMENDATION 2.1 - USE THE SECURITY SOFTWARE OF THE WANG VS SYSTEM TO LOG; A) ALL TRANSACTIONS PERFORMED WITH THE SECURITY SOFTWARE OF THE WANG VS SYSTEM; B) ALL FILES THAT ARE RESTORED TO THE SYSTEM; AND C) LOGONS WITH INVALID OR MISMATCHED USER IDENTIFICATION OR PASSWORDS.

RECOMMENDATION 2.2 - IMPLEMENT A PROCEDURE REQUIRING THE SYSTEMS SECURITY OFFICER TO REVIEW THE COMPUTER SECURITY LOGS ON A DAILY OR WEEKLY BASIS.

The Mission realizes the importance of the security log, particularly as it relates to the controls for the MACS and MACSTRAX systems. However, resource requirement to run this program and other major automation activities has prohibited us from implementing it earlier.

Mission's implementation of the above recommendations would affect the performance of the VS-100 by degrading the already slow VS-100 response time. Further, the Mission will be required to allocate substantial disk storage space to support logs of violations and support the additional workload related to this activity. Nevertheless, Mission is committed to enhance the security controls for MACS and MACSTRAX systems as recommended and has implemented the above recommendations on April 15, 1992.

RECOMMENDATION 3.1 - MODIFY THEIR WRITTEN CONTINGENCY PLAN TO INCLUDE STEP-BY-STEP INSTRUCTIONS FOR RESTORING COMPUTER OPERATIONS FOR EACH TYPE OF DISASTER IDENTIFIED IN THEIR RISK ASSESSMENT.

The Mission's contingency plan, as acknowledged in this report, addressed the following areas as required by the Automation Security Guidebook: 1) identified likely threats that might disrupt computer operations; 2) calculated the intrinsic value of each key system that operates on the Mission's computers; 3) prepared a procedure for making backup copies of the system and data files on the Wang VS system; and 4) identified the sites for moving computer operations in case of short and long term disruption. Although a step-by-step instruction was not included in the occurrence of each likely threat, the contingency plan did provide a standard plan of action in the event of a disaster. Para 3 of the contingency plan designates the Systems Manager and/or any of the ADP staff to trigger the emergency shutdown switch that would shutdown all equipment in the Mission's computer center. Secondly, the plan referred to the Emergency Evacuation of the USAID building, which includes a step-by-step instructions during an emergency.

The Mission has implemented what we think is an excellent backup procedure which is the single most important factor for recovery,

31

We have developed a written agreement with the American Embassy in Islamabad for an alternate processing site in the event of a prolonged disruption. Should all of Islamabad be affected, we have requested USAID Cairo to serve as our alternate processing site. We have two offsite backup locations in Islamabad that maintains a complete weekly backup of all disk volumes for the VS-100 system. As described in the contingency plan, these backup disk volumes would be used in a recovery procedure. Additionally, the Mission sends monthly backup to FA/FM/CAD and the end of year MACS tape.

The recommendation for a step-by-step instructions for restoring computer operations for each likely threat is, in the Mission's opinion, unnecessary. Restoring computer operations after a disaster depends on two factors; 1) a complete backup of the information on the system before the disaster; and 2) a competent staff that would implement the recovery procedure. The specific recovery procedures required for each specific type of disaster requires numerous variables, i.e. the type of disaster, extent of the damage to the computer center, the conditions of each component of the VS-100 system, the availability of funds to procure replacement equipment, developing a schedule for the use of alternate processing sites and/or personnel, etc. Paragraph two of the contingency plan addresses these varied and complex situations in a general sense.

The Mission therefore, considers the ADP contingency plan for its computer resources adequate for restoring computer operations in the event of a disaster. The Mission disagrees with the concept that this plan is ineffective and we are accepting a higher risk than is necessary, without the detailed step-by-step instructions for a recovery.

INTERNAL CONTROLS

Conclusions for Audit Objective No.3

Is the Systems 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?

For this audit objective, the report identified two weaknesses, i.e. user passwords and the security log. The VS user list which contains the passwords for all users on the VS-100 system is accessible only by the System Administrator which is contrary to the report findings. The report implies that other users on the system can read this file and use critical passwords to gain access to the financial and accounting systems which is not true. The VS security program provides the System Administrator access to the user list which enables him to use the security functions of the

32

system to protect access to system resources including the Mission's information database. In 1989, the Mission identified password protection as a possible security weakness because at that time, user passwords were shared among several people within an office using the same logon to access the VS system. This was corrected at the beginning of fiscal year 1990 and all users were provided individual user ids and passwords plus a logon procedure to limit access to the system. User ids are now changed quarterly. Therefore, the 1990 and 1991 Internal Control Assessment findings, determined that the password protection was satisfactory.

The absence of a security log does not mean that the Mission is not protecting its information resources. In fact, there are several levels of protection scheme in place without the security log. First, each user is provided a user id and password to gain access to the VS system. Contrary to the report's finding, the user list which contain user passwords is accessible only by the Systems Administrator. Second, a logon procedure is defined for each user to limit access only to those resources that are required by the user. Third, the Mission is using the Wang file protection class security to limit access to critical files to authorized users, i.e. financial and accounting system files, payroll, etc. For the MACS and MACSTRAX systems, each program has an internal file that controls access to these systems which is maintained exclusively by the Office of Financial Management staff.

The Mission did not implement security logging of violations on the system because of the resource requirement for this program. Our VS system is configured at a maximum level and to run this additional program would severely affect response time and the allocation of substantial disk storage space which was not available.

Conclusions for Audit Objective No.4

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

It is the Mission's position that we have an adequate contingency plan for restoring computer operation in the event of a disaster. The absence of a written step-by-step procedure for each likely threat does not compromise the Mission's ability for recovery. However, we consider that with a good backup system, identified alternate processing sites and a competent staff to implement a recovery procedure, the Mission would be able to restore computer operations in the event of any disaster without any serious delay.

REPORT DISTRIBUTION LIST

	<u>No of Copies</u>
U.S. Ambassador to Pakistan	1
Administrator (A/AID)	2
Mission Director, USAID/Pakistan	5
Assistant Administrator for Asia Bureau (AA/Asia Bureau)	1
Pakistan Desk	1
Asia FPM	1
Office of Press Relations (XA/PR)	1
Bureau of Legislative Affairs (LEG)	1
Office of the General Counsel (GC)	1
Associate Administrator for Operations (AA/OPS)	1
Associate Administrator for Finance and Administration (AA/FA)	1
Office of Financial Management (FA/FM)	1
Management Control Staff (FA/MCS)	2
Financial Policy & Systems Divisions (FA/FM/FPS)	2
Inspector General (IG)	1
Assistant Inspector General/Audit (AIG/A)	1
Deputy Assistant Inspector General for Audit (D/AIG/A)	1
Office of Policy, Plans and Oversight (IG/A/PPO)	3
Office of Legal Counsel (IG/LC)	1
Office of Resource Management (IG/RM)	12
Assistant Inspector General for Investigations and Inspections (AIG/I)	1
Regional Inspector General for Investigations/Singapore (RIG/I/S)	1
Office of Programs and Systems Audit (IG/A/PSA)	1
RIG/A/Cairo	1
RIG/A/Dakar	1
RAO/Manila	1
RIG/A/Nairobi	1
RIG/A/Tegucigalpa	1
RIG/A/Vienna	1
RIG/A/FA	1