

## BIBLIOGRAPHIC DATA SHEET

1. CONTROL NUMBER

2. SUBJECT CLASSIFICATION (695)

PN-AAK-537

TA00-0000-6440

3. TITLE AND SUBTITLE (240)

Survey of computer security for AID's Washington based automated information system

4. PERSONAL AUTHORS (100)

5. CORPORATE AUTHORS (101)

AID / Area Auditor General / Washington

6. DOCUMENT DATE (110)

1980

7. NUMBER OF PAGES (120)

42 p.

8. ARC NUMBER (170)

658.478 A265

9. REFERENCE ORGANIZATION (130)

AG/W

10. SUPPLEMENTARY NOTES (500)

(In Audit report no. 81-26)

11. ABSTRACT (950)

12. DESCRIPTORS (920)

Computer programs  
Computers  
Security  
Automation  
Data processingData storage  
Data transmission  
Audit report

13. PROJECT NUMBER (150)

—

14. CONTRACT NO. (140)

AID/AG/W

15. CONTRACT TYPE (140)

16. TYPE OF DOCUMENT (160)

658.478  
A265

PN-AAK-537

ISN=1813

OFFICIAL FILE COPY



# Auditor General

SURVEY OF COMPUTER SECURITY FOR AID'S WASHINGTON  
BASED AUTOMATED INFORMATION SYSTEM

**Audit Report Number** 81-26

**Issue Date** Dec. 24, 1980

Area Auditor General, Washington  
Agency for International Development  
Washington, DC. 20523

OFFICIAL FILE COPY

SURVEY OF COMPUTER SECURITY FOR AID'S WASHINGTON  
BASED AUTOMATED INFORMATION SYSTEM

TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	1
BACKGROUND	1
SCOPE	3
FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS	3
I. AID Must Establish an Organizational Framework for Addressing Computer Security	4
II. AID Management Must Correct Identified ADP Security Vulnerabilities	8
APPENDIX I - AG/SEC REPORT ON PHYSICAL SECURITY AT THE UNIVERSAL NORTH BUILDING	20
APPENDIX II - LIST OF RECOMMENDATIONS	32

## EXECUTIVE SUMMARY

### Introduction

In 1977 the U.S. Senate investigated the status of computer security in the Federal Government. This investigation revealed a general lack of awareness and concern about the problems of computer security, as well as many cases of serious abuse and misuse of computer resources. In July of 1978, the Office of Management and Budget (OMB) promulgated a Government-wide policy on "Security of Federal Automated Information Systems" (OMB Circular A-71, Transmittal Memorandum #1). This OMB policy requires Federal agencies to develop and implement comprehensive computer security programs.

Within AID, the Bureau for Program and Management Services' Office of Data Management operates the Agency's centralized computer facility, and is responsible for coordinating and assuring the development, implementation and operation of the Agency's computer security program.

### Purpose of Review

The purposes of this review were to:

- Focus management's attention on the problems of automated data processing security and the Office of Data Management's progress in resolving them; and
- Identify computer security vulnerabilities which call for immediate corrective action.

### Organization Improvements Are Needed in the Computer Security Function

The duties and responsibilities of the automated data processing security officer in Data Management are beyond the capabilities of a single individual. Further, although the General Accounting Office has stressed the importance of the security function being independent of computer operations, AID's security function reports through two levels of middle management in the Office of Data Management.

We found that (1) the security computer function is understaffed and has low visibility in the Agency's organizational hierarchy, (2) communication of security information within the Bureau of Management Services and between that Bureau and system users is sporadic, and (3) the Agency has not defined the security duties and responsibilities of computer operators working under contract to the Agency.

### Computer Security Vulnerabilities

AID's computer security needs to be strengthened to assure the integrity of computer information, restrict access to computer information to authorized

users and provide for alternative processing capability in the event of an emergency. We found that:

- Access to AID's automatic data processing systems and data is not limited to authorized users, programs, and processes. For example, user identifications and passwords are changed too infrequently, creating the potential for former employees' continuing to use AID's computer resources. Also, improper disclosure of AID procurement information to prospective contractors is possible. (Pg. 9)
- The use of a specialized computer program capable of modifying programs and data is unmonitored. Although reports are produced for the security function, there is no monitoring of the reports to isolate and investigate possible unauthorized access attempts. (Pg. 12)
- Contingency and disaster procedures for AID's ADP facility are inadequate or non-existent. The Bureau for Program and Management Services has not worked with system users to identify critical data and applications; store that information off-site; assure reliable alternate processing capability; and develop written procedures to minimize the impact of any emergency or disaster at the computer site (Universal North Building). (Pg. 15-17)
- AID management is actively working to improve physical access controls at the computer facility. However, these efforts are hampered by the presence of non-AID tenants in the computer area. Moreover, management has not taken steps to correct identified conditions which increase the possibility of fire and water damage at the computer facility. (Pg. 17)

### Conclusions and Recommendations

Computer security practices in AID do not provide adequate protection over the Agency's computer resources. We attribute AID's poor security measures to a general lack of concern about and commitment to development of a comprehensive program. While some precautions have been taken to safeguard the computer, AID's security program for automated information systems has not received the necessary attention, nor has it been coordinated with all appropriate offices.

We have made 33 detailed recommendations to improve the security of AID's automated data processing resources. These recommendations address four broad areas: organization of the security function, management of the security program, emergency planning, and physical security. The recommendations are included in the text of the report and are listed in Appendix III

### Agency Comments

In responding to this report, officials for the Bureau for Program and Management Services generally agreed with the report. They pointed out, though, that adequate staff and funding have not been allocated nor has higher management supported an effective program. Their specific comments have been incorporated into the report where appropriate.

## BACKGROUND

Managers of Federal agencies are confronted with both Congressional and Executive mandates to protect their agencies' information and control its dissemination.

### Privacy Act of 1974

Congress, through the Privacy Act of 1974 (5 U.S.C. 552a), has imposed numerous requirements on Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. The Act requires that an agency provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of its personal data, whether intentionally caused or resulting from accident or carelessness.

### OMB Circular No. A-71, Transmittal Memorandum #1

The Executive Office of Management and Budget (OMB), which has oversight responsibility for the Privacy Act, determined that there were no specific government policies relating to security requirements for personal, proprietary or sensitive financial data stored and processed by automated systems. It thereupon established a Federal computer security program to guard against improper use of information stored in computers. OMB Circular No. A-71, Transmittal Memorandum #1, issued in July 1978, places responsibility on the head of each cabinet department and independent agency for...

"assuring an adequate level of security for all agency data whether processed in-house or commercially. This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data." <sup>1/</sup>

"It also includes responsibility for assuring that automated processes operate effectively and accurately. In fulfilling this responsibility each agency head shall establish policies and procedures and assign responsibility for the development, implementation, and operation of an agency computer security program."

### 1979 GAO Report

In a January 1979 report, initiated because of expressed Congressional con-

<sup>1/</sup> 'Sensitive Data' is data which requires a degree of protection due to the risk and magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data).

cern over the effectiveness of major Federal agencies' computer security programs, the General Accounting Office stated that Federal agencies, in general, lacked comprehensive computer security programs. They also found that the agencies did not place their computer security functions at a sufficiently high level, with independence from operating functions to preclude preemption by operational priorities.

### AID's Computer Environment

AID utilizes its own computer facilities to process the data used in over 35 of its Agency information systems, ranging from accounts receivable to payroll cost accounting. These facilities which are located in Washington, D.C., process and store personal and sensitive data. Responsibility for developing, coordinating and overseeing an Automated Data Processing (ADP) security program has devolved on the Bureau for Program and Management Services' Office of Data Management (SER/DM). This office provides policy direction for and centralized services in the areas of:

- automated systems required by AID bureaus, offices and overseas missions;
- loan and grant projects which have a data processing component; and
- technical assistance in computer sciences to AID overseas missions.

SER/DM took a first step toward compliance with A-71 by assigning responsibility for ADP security to a management official knowledgeable in data processing and security matters. Also, in February 1979 the office submitted to CMB a highly generalized "Computer Security Plan for AID Automated Information Systems." CMB has not yet responded to this submission.

A 1977 evaluation of physical security for SER/DM, produced by the division's security officer, stated that top management commitment to a well defined plan of action, supported by adequate resources is essential for information privacy and security. In August and September of 1979, Executive Research Associates, Inc. (ERA), at SER/DM's request, performed an assessment to determine AID's ADP security status. The resulting report noted numerous security vulnerabilities and concluded that AID should show greater concern with its ability to provide secure and uninterrupted data processing support to its vital operations.

ERA believed AID's security problems could be directly attributed to inadequate top management commitment, awareness, planning, organization and staffing throughout AID for the security of sensitive and critical automated operations.

Acting on the belief that the February 1979 plan submitted to CMB required greater specificity, AID contracted for and received (from ERA) guidelines for "...initiating the interactions and products necessary to bring AID into full compliance with computer security directives..." These guidelines, delivered to Data Management in June 1980, provide instructions for formulating agency-wide ADP security and contingency plans. Their acceptance by the Agency should, therefore, be an important step toward developing the detailed security procedures demanded by A-71.

## SCOPE

The present limited scope survey builds on the 1979 ERA evaluation. Its purpose is twofold:

- to identify present vulnerabilities which call for immediate corrective action; and
- to bring to the attention of AID management the problems of ADP security and SER/DM's actions to solve these problems.

To meet these objectives, we reviewed:

- compliance with applicable regulations and directions,
- data access controls,
- separation of duties and responsibilities of data processing functions, and
- contingency, disaster and emergency planning.

Our examination included interviews with personnel in the Bureau for Program and Management Services, system users, consultants, and vendor representatives; document reviews; personal observation techniques; and testing of various computer functions via terminals. Since this was a limited scope survey, we interviewed system users in only four organizational units located in two bureaus and one office. Further, testing of various computer functions was limited to elementary checks to avoid any disruption of computer operations.

## FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Computers, and the systems they serve, are assuming an increasingly important and sensitive role in both private and governmental organizations. As dependence on the computer increases, the need to insure that the data contained therein remains accurate, reliable and secure, becomes more acute. As the General Accounting Office has indicated, establishing secure computer facilities and systems assures users that requirements for data confidentiality, integrity, accuracy, and reliability are being met.

AID continues to place increasing demands on its ADP capabilities. The potential damage which can result from unauthorized access to or destruction of data and processing facilities is increasing in equal measure.

Contractor evaluations and in-house studies have identified many of the ADP security problems addressed throughout this report. While the Agency has taken some remedial action to address these problems (e.g., providing full-

time professional security guard service at the computer facility and delivery of consultant-produced security and contingency plans) and has prioritized vulnerabilities (see p 5), SER management has, in general, given low priority to rectifying ADP security vulnerabilities.

Management expresses the attitude that SER/DM is a service organization, existing to serve the interests of AID's ADP users; and operational considerations must therefore take precedence over security when allocating resources. As a result, long-identified security problems remain uncorrected.

## I. AID MUST ESTABLISH AN ORGANIZATIONAL FRAMEWORK FOR ADDRESSING COMPUTER SECURITY

Lacking a sense of urgency, AID management has failed to take the organizational and procedural steps necessary to develop and implement a coordinated ADP security program.

- The ADP Security function, located in the Bureau for Program and Management Services' Office of Data Management (SER/DM), is understaffed.
- ADP security needs have low visibility in the AID organizational hierarchy.
- Communication of security information within SER and between SER and system users is sporadic and inadequate.
- AID has not defined the security duties and responsibilities of computer operators working in SER/DM under private AID contract.

### A. Management Must Review Resource Requirements and Provide Necessary Levels of Support to Meet AID's ADP Security Needs.

The security function within SER/DM currently consists of a Computer Systems Security Officer, who working without a staff, is responsible for developing and coordinating AID's Computer Security Program. This program encompasses physical, administrative, and technical safeguards for the protection of personal and sensitive information and the assets connected with the central computer. A partial listing of the security officer's extensive duties includes:

- Planning, coordinating, and directing the development, implementation, and administration of the computer security program;
- Reviewing security performance through the use of ADP risk assessments, security audits, and analyses;

- Arranging for independent assessment of AID's ADP security posture by outside organizations;
- Monitoring user validation and password processes;
- Developing security procedures for issuance and protection of user passwords;
- Reviewing enforcement of ADP security policy and procedures throughout AID;
- Designing, implementing and monitoring automated security audit trails;
- Establishing and managing a contingency operations program to ensure that SER/DM can continue processing data following a catastrophe at the central computer facility; and
- Performing such other duties as assigned. 2/

Executive Research Associates, Inc., under contract to evaluate AID's ADP security, has expressed the belief that adequate, concurrent attention to all of these responsibilities is beyond the capability of one individual.

The Computer Systems Security Officer stated that he has prioritized his responsibilities and is now devoting most of his time to developing, reviewing and implementing ADP contingency plans (p. 14). Further, during our review, he was assigned to several weeks of temporary duty outside the U.S. As a result, we believe the agency is not producing a balanced effort to upgrade ADP security.

In the Security Officer's opinion, adequate ADP security requires the full time efforts of at least four individuals. One person would develop and implement ADP contingency plans, another would oversee physical security at the Universal North Building. A third person would work with system users, helping them rectify their ADP security problem while the fourth would coordinate implementation of the Agency's Computer Security Plan.

#### Recommendation No. 1

We recommend that the Bureau for Program and Management Services:

- review and analyze the Data Management security function, to

2/ These other duties include extended periods of travel outside the U.S.

determine adequate staffing and support levels, and

— allocate the resources necessary to meet those requirements.

B. ADP Security Should be Coordinated and Elevated Within the AID Hierarchy

The General Accounting Office has recommended that agencies enhance the quality of their effort to upgrade ADP security by establishing -

"...an automated systems security administration organization with independence from computer operations.

This organization should report directly to or through a principal official who reports directly to the agency head and it should have authority to discharge the enumerated responsibilities of agency heads as outlined in OMB Circular A-71." 2/

Responsibility for ADP security and compliance with the OMB security guidelines resides with SER/DM's Security Officer who reports to the Chief of SER/DM's Computer Division (SER/DM/CC). The Chief of SER/DM/CC reports to the Director of Data Management who, in turn, reports to the Assistant Administrator of the Bureau for Program and Management Services (SER). Located deep within the bureaucratic framework of SER, the security function is three steps removed from a principal official who reports directly to AID's Administrator. The present ADP security function is not independent of computer operations. We believe this low visibility contributes materially to Agency management's apparent lack of awareness of and concern about significant ADP security problems.

Recommendation No 2

In order to raise this visibility, and bring the Agency into line with GAO guidelines, we recommend that the Bureau for Program and Management Services establish, coordinate, and oversee an Agency-wide ADP security group or task force reporting directly to the Bureau's Assistant Administrator.

We suggest that the effectiveness of this security group requires the structured participation of all AID offices which have ADP security responsibilities. Some of these AID offices are: the Office of Data Management (SER/DM), the Office of Management Operations (SER/MO), the Office of Public Affairs (OPA), and the Office of the Auditor General (AG).

C. Management Must Establish Channels of Communication for Passage of ADP Security Information Between SER and System Owners/Users

2/ GAO Report to the Congress entitled "Automated Systems Security—Federal Agencies should Strengthen Safeguards Over Personal and Other Sensitive Data", LCD-78-123, January 23, 1979

The Bureau for Program and Management Services develops, coordinates, and oversees ADP security. Adequate security necessitates that system owners<sup>3/</sup> and users assume certain responsibilities. For example, AID's present Automated Information Systems Security plan (dated February 1979) places on data owners and users responsibility for (among other things):

- Compliance with the computer security management control process which includes definition of security specifications and certification of adequacy;
- Ensuring that all sensitive source documents are properly handled, marked and stored to preclude disclosure;
- Determining AID sensitivity to personal or proprietary data to ascertain the degree of protection needed for adequate security;
- Journaling significant events which take place at the user/system level to determine personal accountability;
- Establishing administrative procedures to ensure only authorized personnel with a valid need-to-know can use the system; and
- Establishing physical control procedures to permit access to all areas by authorized personnel while denying access to those who do not have specific need or access authority.

System users we interviewed stated that they were unaware of these responsibilities. Users in the Office of Financial Management (FM) and the Regional Bureaus said Data Management had not contacted them to discuss:

- Security of the facility and system;
- Contingency planning, including evidence and documentation of recent transactions; or
- User responsibilities in the security plan.

We found no evidence that Data Management had asked users to supply information on resuming routine operations in the event of a disaster at the computer center. We question Data Management's ability to adequately plan for contingencies without this input.

### Recommendation No. 3

Since system users we interviewed were not aware of the status of AID's ADP security or their security responsibilities, we recommend that:

<sup>3/</sup> A computer system owner is the primary organizational entity for whom the computer system is developed.

- The Office of Data Management develop, implement, and utilize written procedures establishing on-going methods for periodically informing system owners and users of their responsibilities for data and program security and recovery.

#### Recommendation No. 4

The Office of Data Management develop a policy statement on ADP security for distribution to system users and other affected parties. This statement should explain the importance of computer security, the office's security goals, and the policies and procedures it follows to achieve those goals.

#### D. AID Must Clarify the Security Duties and Responsibilities of Contractor Supplied Computer Operators

Lacking a sufficient number of direct-hire computer operators to perform all necessary processing functions, AID has contracted with a private firm to obtain additional operators. These contractor-supplied personnel often handle all operating functions during non-peak periods, with no AID direct hire personnel present in the computer facility. In an emergency situation, and in the absence of an AID direct-hire, these operators would be expected to act in AID's behalf. For example, they would be required to initiate computer shut-down procedures in the event of an air-conditioning breakdown, and serve as visitor escort for emergency repairmen. In order to maintain control and accountability under such circumstances, it is imperative that the contract operators' legal authority and responsibility be clearly delineated. AID management has not formulated such a definition.

#### Recommendation No. 5

We recommend that the Bureau for Program and Management Services contact and coordinate their activities with the Office of Security (AG/SEC) and Office of the General Counsel (GC) to:

- develop a written definition of contract personnel security responsibilities in the ADP environment, and
- define the status of contract personnel as "representatives" of AID, with authority to act in the Agency's behalf in the absence of direct-hire personnel.

## II. AID MANAGEMENT MUST CORRECT IDENTIFIED ADP SECURITY VULNERABILITIES

We found that AID's ADP vulnerabilities fall into three generalized categories:

- Identification and access controls
- Contingency and disaster planning
- Environmental (physical) controls

A. AID's System of Identification and Access Control Must be Improved

Access control is the process of limiting access to the resources of an ADP system to authorized users, programs, processes, or other ADP systems. AID's existing access controls do not prevent unauthorized access to and use of the Agency's data and equipment. We found that:

- Former employees and contractors familiar with AID's computer system, through the use of computer terminals, can access, modify, or delete information.
- Authorized employees use, without adequate administrative controls, a specialized computer program capable of modifying programs and data.
- Access to the tape library is not consistently controlled, nor are procedures adequately documented (see p 8).

Management Must Implement procedures to Effectively Utilize Present User Identification, Passwords, and Specialized Software Controls

Because of inadequate access controls, improper disclosure of AID procurement information to prospective contractors is possible. System users identified four information systems with data bases containing financial data. Three systems users concluded that these financial data could be of value to prospective AID contractors.

Prospective contractors could gain access to these data because of two access control deficiencies:

- the infrequent changing of user identifications and passwords, -and
- the visual displaying of passwords on the cathode-ray tube terminals.

Access to AID's computer system via a terminal requires a valid user identification\* and password combination, and a telephone number. The purpose of the identification and password combination is to deny access to unauthorized users. Because user identifications and passwords are infrequently changed, former employees and prospective contractors familiar with AID's computer system could easily gain access to AID's information systems.

---

\*A user identification is a symbol composed of six letters or numbers that identifies the system user to the computer operating system.

The Information Management Division of Data Management is responsible for controlling and changing user identification. Information Management Division officials knew of no documented policy on when to change or delete user identifications; but they said that when a new DM analyst is assigned responsibility for an established system, the user identifications for the system are changed and the old identifications deleted. Of the system users we interviewed in the Regional Bureaus, one said that user identifications are not changed when a knowledgeable person leaves AID. The other user did not see a need to change user identification under any circumstances.

During the course of this survey, the Information Management Division updated an internal directive on the changing and deleting of user identifications.

According to Data Management, system users are responsible for controlling and changing their passwords. When the passwords in conjunction with user identifications limit access to security protected computer resources, system users and their Data Management counterparts have the capability to change the passwords. However, when the passwords together with user identifications allow system users access to the computer system and not to specific protected computer resources, only Data Management personnel can change the passwords. During our survey we asked the three system users in the Bureaus to explain their method for changing passwords. They all said they would ask Data Management personnel to change the passwords, although two of the three thought they had the capability to change the passwords themselves. In any event, passwords are changed infrequently. One of the system users changed the passwords through Data Management personnel three months prior to our review. The other two users said their passwords have not been changed in over a year.

AID's control over passwords is weak for the second reason. According to the Computer Center User's Guide, the password will be "masked out" when logging on (to the system), so that there is no potential for an unauthorized person's seeing it and then using it to gain access. In actuality, passwords appear on the cathode-ray tube (CRT) terminals. The computer programs controlling an individual user's access to the system were designed for use with the printing-type terminals. When these programs were used, a mask composed of random characters was generated on the terminals, and the system user typed the password into the mask, preventing visual disclosure of the password. However, technical and operational characteristics have changed with the installation of CRT terminals. On these terminals, only a single character can occupy a given space on the CRT terminal's screen. When a mask of random characters is generated and the password is entered, the random characters are replaced by the password. Neither the old

program nor the procedures for communicating between CRT terminals and the central computer facility were modified to prevent this visual disclosure of the password.

### Capabilities of the User

These access control deficiencies are extremely important, because any user of the system, authorized or unauthorized, can perform a variety of tasks. We tested several possible system functions and verified that system users can:

- read the contents of computer files belonging to other system users;
- delete computer files belonging to other system users;
- copy computer files belonging to other system users; and
- replace computer files belonging to other system users with computer files containing bogus information.

These tests were performed using the Time-Sharing Operating System (TSO) on non-security protected computer files belonging to the Bureaus and to system C446 (Cost Accounting) and system C447 (Travel Advance accounting). Further, TSO does not allow system users to execute these functions against Index Sequential Access Method (ISAM) and direct access method (DA) files.

The Agency's use of user identifications and passwords does not prevent access to its data and systems by un-authorized persons. Since (i) an unauthorized person can perform a variety of tasks, and (ii) AID's computer files contain information of value to prospective contractors, we believe that control over access to AID's computer files must be tightened.

### Recommendation No. 6

To improve utilization of user identification as an access control, we recommend that Data Management change those user identifications periodically, but no less frequently than whenever a Data Management staffperson familiar with a system and its data bases leaves his/her position of responsibility.

### Recommendation No. 7

Since system users seldom change passwords, Data Management must assume responsibility for their control. We recommend that Data Management:

- change passwords assigned to critical and sensitive applications every 6 months or when someone knowledgeable of the password no longer has a need to know;

- change passwords assigned to all other applications every 12 months or when someone knowledgeable of the password no longer has a need to know, and
- require system users to notify Data Management when someone knowledgeable of the password no longer has a need to know.

#### Recommendation No. 8

To improve control over password dissemination, we recommend that Data Management modify either the programs or the communication procedures to prevent visual observation of the passwords on the CRT terminals.

#### Resource Access Control Facility

A control program is available to Data Management to assist in protecting AID's ADP resources: Resource Access Control Facility (RACF), IEM's proprietary product, is a control program that provides for integrity related to the use of or access to data files. Within AID, however, RACF is underutilized and unmonitored. Our questioning of three Bureau users and the Office of Financial Management revealed that only Financial Management was protecting computer files with RACF. When two users were asked about RACF, one said the opportunity to choose to use RACF had not been offered; and the other had never heard of RACF. Also RACF has an audit attribute which allows responsible officials to obtain reports showing attempted accesses. Although the reports are produced for the security function, there is no monitoring of the reports to isolate and investigate possible unauthorized access attempts.

#### Recommendation No. 9

To improve RACF utilization, we recommend that:

- The Bureau for Program and Management Services require that all critical and sensitive applications be protected by using RACF.
- Data Management monitor reports produced by the audit attribute of RACF which show attempted accesses to RACF protected applications; isolate and investigate unauthorized access attempts.

#### "AMASPZAP"

AID has not established adequate administrative controls over the use of a specialized computer program called AMASPZAP. This IEM program, which was first developed in 1968, was intended as a problem-solving tool. It enables system programmers to bypass standard operating procedures and quickly modify data and programs. In a 1979 evaluation, consultants reported that this program enables system programmers to

bypass security features and make changes to a program, change the Volume Table of Contents of a disk pack, and make direct modifications of data in a file. The ERA consultants concluded that the use of AMASZAP ...

"should be strictly controlled and limited to the use of as few individuals in Software Management Branch as is operationally possible. Formal procedures should be established in writing and should be enforced to assure accountability..."

Further, ERA, Inc. representatives said this capability should be password-protected.

Data Management officials told us this is not a significant problem, since (i) only the system programmers have access to the program, (ii) a log is kept of the changes made to the system, and (iii) the capability is now RACF protected. They noted however, that a separate report on AMASPZAP utilization was not maintained.

We discussed the capabilities of this program with IBM representatives and they agreed with the consultant's conclusions.

#### Recommendation No. 10

Data Management should control the use of AMASPZAP by establishing written procedures for documenting and justifying each use of AMASPZAP.

#### 2. Management Must Establish Written Procedures Limiting Access to the Magnetic Tape Library and Protecting its Sensitive Contents

In the absence of an off-site storage facility, the magnetic tape library located adjacent to the computer room, is the sole repository for Data Management's primary inanimate asset, its data. We could find no written procedures (i) limiting computer operator access to the library or (ii) describing obligations of computer personnel and precautions to be used in the library or computer room during the physical handling of data subject to the Privacy Act. Recording media, e.g. magnetic tape, are not marked for special protection. We found no current listing of systems containing information subject to the Act.

During the primary operating shift, an AID direct hire librarian, we were told, controlled access. However, contract personnel often operate the computer facility during non-peak hours in the absence of Agency direct hires (see p 8). During those periods, the contract operators have free and uncontrolled access to the library.

#### Recommendation No. 11

We recommend that:

- The Office of Data Management develop and implement written procedures to control access to the tape library and track the movement of magnetic tapes. These should include a logging procedure to record all movement of tapes into or out of the library.
- The Office of Data Management review its personnel scheduling procedures to consider the feasibility of providing that at least one AID direct-hire employee is in the computer area during all operating shifts. While on duty, this employee should serve as tape librarian with sole access to and control over the library.

### Recommendation No. 12

Following an inventory to identify media (magnetic tapes and disks) containing "sensitive" data and programs, the Office of Data Management should develop and implement written procedures to provide special protection for such data. These procedures should include a description of duties and responsibilities of personnel handling such data; color coding of the media containing these data; and a maintenance of up-to-date hard copy authorization list of all individuals (computer-personnel as well as system users) allowed to access the data. We recommend that management utilize the official guidelines detailed in the National Bureau of Standards' Federal Information Processing Standards Publication 41 in developing these procedures.

### B. AID Management Must Improve Contingency and Disaster Planning

Despite the most assiduous application of precautionary measures, there always remains some possibility that events will occur in a computer facility which could hinder or prevent normal processing operations. Fire, water or other damage at the facility could bring automated data processing to a complete halt.

Adequate security necessitates three types of contingency plans, as described in the National Bureau of Standards' Federal Information Processing Standards, Publication 31.

- Emergency response: written procedures for response to emergencies such as fire, flood, civil commotion, natural disasters, bomb threats, etc., in order to protect lives, limit the damage to property, and minimize the impact on ADP operations.
- Backup operations: agreements and procedures to insure that essential tasks can be completed subsequent to disruption of the ADP facility, and critical operations can continue until the facility is restored.

— Recovery: written procedures to permit smooth, rapid restoration of the ADP facility following physical destruction or major damage.

Yet we found portions of AID's current overall contingency and disaster planning to be outdated, incomplete, or unimplemented.

1. AID Management Must Review and Update Current Emergency Response Plans for the Universal North Building

Emergency response planning refers to steps taken immediately after an emergency occurs to protect life and property and to minimize the impact of the emergency. These steps, some of which SER/EM has outlined in internal memoranda, should be included in a facility "Self-Protection Plan", as required by AID Handbook 20. The current self-protection manual for the Universal North Building is both outdated and inadequate in content.

The Universal North Building Facility Self-Protection Plan contains basic emergency procedures to be followed by building occupants in the event of fire, explosion, bomb threat, or other civil or natural disturbances. It also contains a listing of duties and responsibilities for personnel on each floor of the building. Published in September 1976, the Plan is outdated and incomplete. SER/EM officials told us that more than 50% of the personnel listed in the current plan as wardens, assistants and monitors for the 7th floor no longer reside on that floor. Further, the plan is incomplete because it fails to address special needs of the ADP facility such as protection of equipment during a period of civil commotion or control of data and hardware loss after a fire or flood.

Under current Agency procedures, establishment and implementation of a building self-protection plan is the joint responsibility of the Agency Safety Office, within the Office of Management Operations (SER/MO), and the senior AID official occupying the building. For the Universal North Building, this official is the head of the Office of Financial Management (Controller).

Recommendation No. 13

We recommend that:

- The Chief, General Services Division of the Office of Management Operations (SER/MO/GS) and the Controller, Office of Financial Management (FM), coordinate their activities and implement established procedures to produce a comprehensive building self-protection plan, contained in an up-to-date manual, for the Universal North Building.
- The Office of Data Management identify emergency conditions and procedures which have particular implications for ADP operations, such as protection of equipment during a period of civil commotion or loss of control subsequent to a fire, flood, etc. In order to consolidate instructions, these procedures, some of which have already been published in internal EM memoranda, should be included

possibly as amendments, in the revised Building Self-Protection Manual.

2. Management Must Provide Adequate Back-up Storage and Processing Capability For Critical Data and Applications

We believe that the lack of contingency plans and procedures for back-up and recovery of ADP capability to be the most immediate and pressing computer security problem facing Agency management. At the present time, an emergency at the computer facility could shut down AID's computer processing capability for an indefinite period. Back-up operations include:

- selection of an off-site storage for retention of magnetic tapes containing data and programs considered essential for continued Agency operations,
- selection of an alternate processing site to "run" those critical programs, and
- written procedures to facilitate smooth transfer of operations to the alternate processing site.

SER/DM together with users have not inventoried and ranked their data and programs to determine which are critical for continued Agency operations, but they have begun storing some critical back-up tapes at a designated alternate storage site. SER management must work with system users to identify critical information and store it off-site.

Recommendation No. 14

We recommend that:

- Data Management and users develop procedures for identifying and ranking critical data and applications.
- The Office of Data Management develop written instructions to system users detailing their responsibilities in reconstructing data files following damage to or destruction of Data Management records.
- The Bureau for Program and Management Services, in conjunction with system users, develop and implement written procedures detailing action to be taken and fixing responsibilities for back-up operations in the event of temporary or permanent damage to the computer center.

In addition to providing off-site storage of critical data and programs, the emergency back-up procedures must identify an alternate processing site to run the critical programs. AID has entered into an agreement in principle (not a binding contract) with the Department of State for mutual emergency computer processing back-up support. Neither organization has attempted to "run" their programs at the other's facility. Further, SER/DM officials stated that technical incompatibilities between State Department

and AID systems make this agreement impractical. They are, therefore, studying alternative methods for providing back-up processing. As a result, AID presently has no back-up processing capability.

Moreover, the Agency has no written procedures to facilitate or implement a transfer of processing operations to the alternate site as suggested in Federal Information Processing Standard Publication No. 31 dealing with back-up operations planning.

Any prolonged shutdown of processing capacity at Universal North would necessitate alternate site processing. The present, non-contractual agreement with the Department of State for mutual back-up processing was a first step in assuring such capability. AID management cannot assume such a capability exists, however, until the Agency has developed and adopted written procedures for transferring such operations, and demonstrated an ability to process data at the alternate site.

### Recommendation No. 15

We recommend that:

The Bureau for Program and Management Services should continue to develop a back-up processing plan following the guidance provided in the National Bureau of Standards' Federal Information Processing Standard Publication No. 31, Section 8.3.

### 3. Management Must Develop and Implement Procedures to Expedite Recovery Operations at the Principal Computer Facility

The use of a back-up facility usually occasions both extra expense and downgraded performance. Management should, therefore, develop a set of procedures minimizing the time required to bring a central computer facility back into operation.

SER/DM has not developed such a recovery procedure.

Recovery from total destruction will require:

- locating and obtaining possession of enough floor space to house the ADP facility;
- performing required physical modifications (e.g., air conditioning, partitions);
- procuring and installing computer hardware;
- procuring needed office supplies, and
- verifying that all needed hardware, equipment and materials are on hand and in good working order and then transferring operations from the back-up site(s) to the reconstructed computer facility.

Written guidance for carrying out these tasks would facilitate renewed operations.

Recommendation No. 16

To facilitate recovery operations following an emergency at the central computer facility, we recommend that the Office of Data Management formulate and implement recovery procedures based upon the guidance contained in the National Bureau of Standards Federal Information Processing Standards Publication 31.

C. Management Must Improve Physical Security in the Computer Area

Physical security of the computer facility includes:

- controlling access to the computer area, and
- providing a safe working environment within the computer area.

AID's Office of Security (AG/SEC) has reviewed the physical security within AID's computer area, and their detailed report is contained in Appendix I.

We found that AID management has taken positive steps to provide better access control but has failed to rectify many long identified environmental problems within the computer area.

Physical access controls have been improved with the assignment of a full-time security guard to the 7th floor of the Universal North Building, where AID's computer installation is located. However, the presence of non-AID and non-U.S. Government tenants on that floor presents a significant impediment to implementation of improved security procedures. For example, attempts to improve identification procedures for computer personnel must consider the fact that non-AID tenants cannot be required to display AID issued identification badges.

Inadequate environmental safeguards compound the potential for fire and water damage to the computer area. The overhead water sprinkler system, for instance, fails to provide coverage of the computer paper storage room directly adjacent to the computer room. Further, the sprinkler system, installed in 1977, has never been inspected or tested. There are no detectors to warn of water leakage under the computer rooms raised flooring (an area of criss crossing electrical and communications wiring).

SER/DM submits building services requests to SER/MO for transmittal to the General Services Administration (GSA). SER/MO officials told us that SER/DM had submitted requests for water detectors and sprinkler inspection. The former was submitted in December, 1979. SER/MO has not yet forwarded the request to GSA, as they are waiting for GSA to perform a computer room water damage survey which SER/MO first requested in November, 1979. Neither SER/DM nor SER/MO were able to tell us when SER/DM requested a

sprinkler inspection.

We believe management must take immediate steps to correct these and other problems as noted in Appendix I.

Recommendation No. 17

Physical security provides the most basic form of ADP protection.

We recommend that:

- The Assistant Administrator of the Bureau for Program and Management Services, in coordination with the General Services Administration, explore available alternative courses of action and intensify efforts to remove all non-AID tenants from the 7th floor of the Universal North Building.

## APPENDIX I.

### AG/SEC REPORT ON PHYSICAL SECURITY AT THE UNIVERSAL NORTH BUILDING

#### I. Introduction

##### A. Area Surveyed:

Office of Data Management, seventh floor, Universal North Building

##### B. Address:

1975 Florida Avenue, N.W., Washington, D.C.

##### C. Period of Survey:

July/August 1980

##### D. Ownership/Management of Property:

Ownership: Universal North Incorporated

Managed: Cafritz Realtors, 1825 K Street, N.W., Washington, D.C.  
Phone: 667-4410

#### II. Environmental Background - Universal North Building

##### A. Structure

The Universal North Building is a twelve story, reinforced concrete, brick and glass structure with a class A fire rating. The building is triangularly shaped and borders Connecticut Avenue, Florida Avenue, and T Street in Northwest Washington, D.C.

##### B. Entrances

There are three main entrances into the Universal North Building:

- 1975 Florida Avenue,
- 1875 Connecticut Avenue, and
- 2024 T Street.

Entry may also be gained from the attached garage on the G-1 and G-2 levels. Entry from the garage is conditional upon possession of a key issued by the building management. Occasionally the door may be found ajar. Given the number of keys that are outstanding, it is reasonable to assume that the integrity of the key control system has been compromised.

### C. Operating Hours

The Connecticut and Florida Avenue entrances are open from 7:00 a.m. to 6:00 p.m., Monday through Friday. The T Street entrance is open from 7:00 a.m. to 11:00 p.m., Monday through Friday. The building is secured on weekends and holidays. Garage hours are 6:30 a.m. to midnight.

### D. Building Security

Cafritz provides building security through a contract with Security Incorporated, 5518 Dorsey Lane, Washington, D.C. Phone: 301-656-6800. As a part of the contract, Central Security (298-7310), a subsidiary of Security Incorporated, has installed an electronic card access system in the building for use during security hours. The Connecticut and Florida Ave. entrances are manually locked by building maintenance personnel at 6:00 p.m., Monday through Friday. The T Street entrance is electronically controlled during the hours 11:00 p.m. to 7:00 a.m. A direct line telephone is co-located with the card reader on the T Street entrance in case of emergency or a need for assistance.

All entrances are alarmed and tied to the Central Security system. From 6:00 p.m. to 7:00 a.m., Monday through Friday, and twenty-four hours a day on weekends and holidays, elevators off the T Street entrance must be called via an electronic card reader. Once in the elevator, floor movement is not controlled.

The building security system provides an option for local alarms to individual suites. The option was declined by AG/SEC due to existing security

Complaints from Data Management personnel concerning the building access system are frequent, and generally concern malfunctioning cards or card readers and a lack of response to telephonic queries for assistance. Repeated AG/SEC notifications concerning these problems to both the building management and Central Security have not resulted in noticeably improved service.

The Universal North Building is located in Police Precinct #3 and is covered by Fire Station #9.

### E. Tenants

Universal North is a multi-tenanted office building housing a large number of small private professional offices and a variety of public and governmental organizations. Noteworthy tenants other than AID include: The American Cancer Society (Room 1018); the Arab Information Center (Room 1110); the Arab League Special Envoy (Room 1016); The Civil Aeronautics Board (Room 1034); District of Columbia Office of Human Resources (Room 415); The Embassy of Spain Industry and Energy Office (Room 1020); The Federal Housing Administration (Room 1240); The Hilton Hotel Corporation (Room 1214); The Internal Revenue Service (Room 432); The Social Security Administration (Room 708), and the Japanese American Friendship Commission (Room 709).

## F. Surrounding Area

The Universal North Building is surrounded by a conglomeration of apartments, private residences, small business establishments, and the Hilton Hotel.

## G. Protective Lighting

### 1. External lighting

Universal North Building has no external lighting system. Adequate lighting is provided through street lights and surrounding commercial establishments.

### 2. Internal Lighting

Spaced throughout the building in corridors, lobbies and stairwells are lights which remain on on a twenty-four hour basis. In addition, the stairwells have emergency backup lights which are supported by rechargeable batteries and designed to activate with a break in normal current. These lights are periodically tested by the building management.

## III. Physical Security of Data Management Area (7th floor; Universal North Building)

### A. Access/Locks/Alarms

There are five possible means of access onto the 7th floor.

#### 1. Main Entrance:

Doors - double: lead from elevator lobby to main corridor.

Lock - Yale 197 1/4

Open - Flexitime duty day

Alarm - ADT contacts: to local panel in 5th floor guard post.

#### 2. Secondary Entrance:

Doors - double; lead from elevator lobby to Room 737

Locks - Simplex

- Yale 197 1/4

- Cipher with battery backup and brute lock

Open - with simplex combination during flexitime duty day

Alarm - ADT contacts to local panel in 5th floor guard post.

(Note: Cipher lock system is not in use. A 1978 work order to GSA for needed electrical socket has not been honored)

3. Service Elevator:

Doors - double; lead from elevator to main corridor

Locks - 181 deadbolts at top and bottom of stationary door

- Yale 197 1/4

- Cipher with battery backup and brute lock

Open - As needed basis

Alarm - ADT contacts to local panel in 5th floor guard post.

(Note: Cipher lock system is not in use. A 1978 work order to GSA for needed electrical socket has not been honored.)

4. Emergency Stairwells (2):

Doors - double; lead from stairwells into main corridor

Locks - 181 deadbolts at top, bottom and center of stationary doors

- key in knob

- Cipher with battery backup and brute lock

(Note: Cipher lock system is not in use.

A 1978 work order to GSA for needed electrical socket has not been honored.)

Open - exit only during flexitime duty day

Alarm - ADT contact to local panel in 5th floor guard post.

B. Guard Force

The current guard contract with Atlas Security is provided through the General Services Administration (G.S.A.). Atlas Security is located at 3461 North Washington Boulevard, Arlington, Virginia. (phone 703-243-7676/77/78). The main guard office at Universal North is in Room 515 (632-0039). The 7th floor guard post (Phone 632-5386) is located in the main corridor directly off the elevator lobby and is by contract a twenty four hour, seven day a week operation. Monday through Friday from 6:30 am

to 10:30 pm, there is also a roving guard whose functions entail providing relief breaks and assisting in 7th floor guard responsibilities.

The GSA transition to Atlas Security was hampered by inadequate guard company personnel and clearances. In addition GSA failed to provide the necessary guard orders.

Data Management personnel have reported deficiencies in guard company performance which have adversely impacted on their operations. Efforts to correct these deficiencies have resulted in the dismissal of five guards from the building and letters to GSA requesting their assistance and, if necessary, the termination of the contract.

### C. Internal Personnel Controls

During the normal work day, employees with AID, State, IDCA, or authorized contractor ID cards are granted access to the 7th floor main corridor through display of their ID cards. Visitors must sign the guard registry, announce the purpose of their visit, and be escorted by an employee of the appropriate office involved. Those personnel with the combination to the Simplex lock on Room 737 may bypass the guard and gain entry through that door. During security hours, all persons with authorized ID cards must sign in and visitors must continue to be escorted. The east wing of the main corridor on the 7th floor has been designated a controlled area and personnel within this area are to display a valid ID card at all times.

Representatives from the Social Security Administration and the Japanese American Friendship Commission currently bypass the guard without showing identification. The Japanese American Friendship Commission has indicated a willingness to move assuming all expenses are incurred by AID. The Social Security Administration has tentatively agreed to display ID cards to gain access to the floor and to have their unannounced visitors escorted when stricter procedures are implemented.

Members of the cleaning and maintenance crews are given Cafritz ID cards. They are required to sign in the visitors log and are escorted whenever possible. The current Cafritz cleaning contract is with Ship Shape Maintenance Company, 2254 25th Place, N.E., Washington, D.C. No security checks are run on members of the cleaning crew due to the high turnover in personnel.

- D. The facility self-protection plan is outdated and in need of revision. While AID responsibility for it rests with the Agency Safety Officer, specific assignments are delegated to building occupants. Current building coordination responsibilities rest with Financial Management. Per agreement between Data Management and Financial Management, this responsibility will shift to Data Management with the relocation of the main guard office from the 5th to the 7th floor.

Fire drills are held periodically by AID Management. The last scheduled drill occurred in October of 1980 and indicated a problem with alarm audability in

the computer room and parts of the 7th floor. Earlier, on August 25, 1980, a small fire resulted in an evacuation of the building. Although guards notified offices within DM, personnel within the computer room neither heard the building alarm nor were notified by floor wardens. The fire was extremely minor and no injuries or significant damage was incurred.

#### Recommendation No 18

We recommend that the safety officer in the Office of Management Operations coordinate with GSA to insure immediate installation of a fire warning system which can be heard throughout the entire 7th floor.

#### IV. Procedural Security

The Office of Data Management participates in the agency's principal/unit security officer program. Currently the principal security officer is Lucille Murphy and the unit security officer is Stanley Mashakas. Data Management has a total of 22 bar lock cabinets which house primarily Limited Official Use/ Privacy Act information. Classified information is virtually non-existent within Data Management. All mail (classified, LOU, Privacy Act information, and unclassified) is transported between the State Department Building and Universal North by regular SER/MO couriers. Pickup and deliveries are made to the Communications and Records Center, Room 536.

##### A. Security Aids

Few security posters were evident throughout the Data Management area.

##### B. Classification Authority

There are no authorized classifiers within the Office of Data Management. Its Director, however, is authorized to downgrade and declassify.

#### V. OMB Transmittal Letter A-71

As a result of OMB Circular A-71 and subsequent requirements issued by GSA and the Department of Commerce, remaining attention within this survey is addressed specifically to the computer, the computer operation, and factors impacting on their physical security.

##### A. Threat Assessment

It is AG/SEC's belief because of the generally non-controversial nature of the Agency, the low Washington profile AID maintains, and the availability of far more prestigious targets in the immediate area, that the probability of a specific outside threat being directed against the Computer Center is extremely low. It is further believed that any incident involving physical damage to the computer will be the result of unrelated activities occurring within the building. Such factors are to a certain extent uncontrollable

in leased space. The results of such an incident upon the Agency would indeed be significant, however, and the impact would extend well beyond the dollar loss of equipment involved.

There are no known threats being directed against the facility at this time. If, in the future, a significant long term threat should develop, there would be no recourse other than a significant increase in existing security or a transfer of the computer to another facility.

AG/SEC believes a less costly but more realistic potential problem area rests with the unauthorized use of the computer or its data base by employees, contractors or persons knowledgeable of its systems.

## B. Communications

Communications between Data Management and AG/SEC have increased markedly since OMB A-71 discussions were resurrected in 1980. There does exist, however, a communication problem which stems from a lack of procedural guidelines and insufficient communication between offices. This frequently results in matters being addressed when they reach crisis proportions rather than as they occur. There is a need for employees and contractors alike to be made aware of the need to advise management and AG/SEC, on a timely basis, of those security-related matters that are in need of correction. Secondly, an agreement is needed between Data Management and AG/SEC that all instructions for the guard force will be provided by AG/SEC. Individual instructions from non AG/SEC personnel results in confusion on the part of the guards and can result in conflicting instructions from different offices. Paralleling this is a need to raise the level of awareness of non-management Data Management personnel that their efforts are required if there is to be an improvement in Data Management security.

### Recommendation No. 19

We recommend that Data Management consider the development of an orientation program for their personnel which would instill an awareness of the need for security, advise them of the security-related procedures to be followed, and cite the appropriate chains of command to discuss security-related problems.

## C. Guard Force

The GSA is the agency responsible for contracting guard forces within the Federal Government. As a result, AG/SEC has minimal input into guard company selection, guard hiring procedures, and guard instruction and training. There exists, therefore, a need to identify, in the simplest of terms, the procedures and functions expected of the guard force, and to design a system to insure compliance.

### Recommendation No. 20

Representatives from Data Management and AG/SEC should continue to coordinate

and co-author additional instructions as necessary on procedures for (1) emergency access, (2) patrol procedures, and (3) fire and smoke detector response.

#### D. Access Controls Within Data Management

Access procedures to and within the 7th floor are inconsistent and ineffective. Currently, representatives from the Japanese American Friendship Commission and the Social Security Administration Office are permitted entry without challenge, while AID employees and contractors entering the main corridor must display a valid ID card. Guards are to contact Data Management personnel for escorts for visitors to controlled areas while visitors to the Japanese American Friendship Commission and the Social Security Office are permitted free passage. Across the elevator lobby from the guard desk, Data Management employees and contractors with the combination to the Simplex lock gain unchallenged access to Room 737 and connecting offices. Unauthorized personnel who choose to tailgate may also enter Room 737. As a result, AG/SEC is exploring the feasibility of closing doorway 737 as an elevator lobby access point and equipping it with panic hardware which would permit egress in an emergency.

Upon entry into Room 737, there exists a possibility of unchallenged access to the schedule and control area. While there is a 181 Deadbolt on the interconnecting doorway between these two rooms, it is frequently left open for employee convenience. Further, if it is closed in accordance with the prescribed procedures, this interconnecting door which is locked on and opens into the schedule and control area takes on the dimensions of a serious fire hazard. This is because the peculiar design of the building has both emergency stairwells located on the same side of the elevator lobby. In the event of a fire in the vicinity of the elevator lobby or the guard desk, access to an emergency exit may possibly be denied to personnel in the west wing of the building. Panic, serious injury, or even death could result. It is an unacceptable presumption to assume that an individual in Schedule and Control would be present or have the presence of mind to unlock this interconnecting door to permit an alternate means of egress.

Paralleling the main corridor on the T Street side of the building is an inner corridor which runs basically the entire length of the building. Although Data Management offices on the main corridor are equipped with either Simplex or key in the knob type locks, and procedures call for these doors to remain locked, one can generally find an open doorway.

On occasions, guards have reported instances of noncleared personnel attempting to bypass access controls by turning left at the guard desk as if going to the Social Security Office, and then entering an unlocked AID office on the right. In doing so they gain access to the inner corridor and can thus circumvent the guard into the controlled area. Because of this breakdown in security procedures, access is granted to the east wing controlled area.

### Recommendation No. 21

In conjunction with the AG/SEC proposal to close doorway 737, we recommend that Data Management consider alternative plans for means of entry into 737 which would also incorporate fire safety considerations.

### Recommendation No. 22

We recommend that representatives from AG/SEC, SER/MO and Data Management continue to meet with personnel from the Social Security Administration and the Japanese American Friendship Commission for purposes of formulating a written agreement defining acceptable identification access procedures and controls for the 7th floor.

### Recommendation No. 23

We recommend that Data Management identify their areas by function/equipment sensitivity and that access to those areas deemed sensitive be controlled by an electronic card reader system and physical barriers.

## E. Fire Safety

The AID computer room is equipped with smoke detectors and dry pipe sprinklers that are independent of the building fire safety system. Currently the smoke detection system is inspected by GSA on a periodic basis. Data Management recognizes the need to have the sprinkler system inspected periodically as well. Data Management efforts to have a Halon Fire Extinguishing System installed have been frustrated by GSA.

There are two multi-purpose, one water, and six carbon dioxide fire extinguishers throughout the computer room, storage area and tape library. The carbon dioxide extinguishers were last checked January 17, 1979. The first multi-purpose extinguisher was inspected November 27, 1979, and the second on January 18, 1979. The water fire extinguisher was checked January 18, 1979. While the positioning of the extinguishers within the computer room is generally good, they are hung at such a level as to not be readily visible. In addition, the carbon dioxide extinguisher in the tape library is positioned on the rear wall of the room. For one to gain access to it during a tape library fire, it would be necessary to pass through the room and the fire to the extinguisher:

Immediately adjacent to the computer room and connected by a doorway is the computer supply room. This room is equipped with smoke detectors, but not a sprinkler system. While the location of the storeroom is obviously convenient for computer room employees, we believe the combustible materials stored therein represent a significant fire hazard to the computer room operations.

Currently, the main corridor door into the storeroom is secured with a 131 Deadbolt and combination padlock. This procedure precludes the entry of emergency personnel into the area by any means other than the computer room.

Transformers for the computer are located in a small air conditioned room within the computer center. These transformers receive their power directly from Pepco. One transformer within this room was found to be humming excessively

and was so hot, one could not rest a hand on it. Data Management had the additional equipment available to alleviate the problem but its installation was delayed by GSA. It has since been installed and approved.

At various doorways within the computer center are emergency shut-down plungers which interrupt current between transformers and the computer. Based on our inspection of the transformer room noted above, we believe a likely point for fire is the transformer room itself. Within the computer room and immediately adjacent to doorway 733 is a panel which indicates the smoke detectors that have been activated. In addition, a map has been drawn by Data Management personnel indicating the location of the smoke detectors beneath the floor and their corresponding panel designations. Unfortunately, a copy of this map is not located at the panel itself.

According to records maintained in the computer room, only four computer room personnel have been trained in the use of the carbon dioxide fire extinguishers. This training occurred in 1977. Neither members of the guard force nor contractor personnel have received any training.

#### Recommendation No. 24

We recommend that the Safety Officer in the Office of Management Operations:

- post signs clearly reflecting the placement of fire extinguishers;
- have the fire extinguishers inspected and replenished as needed; and
- relocate the fire extinguisher in the tape library to a more accessible area.

#### Recommendation No. 25

We recommend that the Safety Officer in the Office of Management Operations schedule training for Data Management employees, contractors and guard force personnel in the use of extinguishers and general fire fighting techniques

#### Recommendation No. 26

We recommend that the Safety Officer in the Office of Management Operations request a certified electrician review the emergency shut-down plunger system to determine the feasibility and advantages of an electrical current interruption system, located at a point before the transformer.

#### Recommendation No. 27

We recommend that the Safety Officer in the Office of Management Operations clearly mark the location of smoke detectors with numbers corresponding to the wall panel.

#### Recommendation No. 28

We recommend that the Safety Officer in the Office of Management Operations

consider requiring the relocation of storage room materials to an area which would minimize the impact of a storage room fire upon computer operations.

#### F. Contractors

Federal Personnel Manual Systems (FPM) letter 732-7 dated November 14, 1978, states that contractors assigned to the computer related activities within the Federal Government must have their position designated ADP 1, 2, or 3, in accordance with the position's sensitivity and its impact on policy. Current DM contract positions have now been identified in accordance with this requirement and investigations are being initiated.

These investigations, since they are for non-competitive positions, can be conducted by AG/SEC rather than by the Office of Personnel Management.

Inconsistencies exist within Data Management about contractor access to the computer facility. During the normal duty day, contractors are not allowed escort privileges within Data Management nor are they allowed access to the tape library. During evenings and weekends, however, these same contractors are not only granted access to the tape library, they are left in charge of the entire facility.

Computer Center Division personnel expressed preference for Data Management personnel to be present during all shifts. While this is not being done because of apparent personnel shortages, we believe Data Management recognizes the desirability of greater controls over contractors in the computer operation.

Section 975.3-2 of the Uniform Security Regulations deals with contractors and access to AID facilities after duty hours. Specifically, it precludes their presence without direct-hire escort.

#### Recommendation No. 29

In view of the potential problems surrounding Data Management's need for twenty four hour contractor support and the resulting conflict with existing security regulations, we recommend that Data Management either comply with the regulation or justify and formally request exception to the regulation which requires direct hire oversight of contractors working within AID facilities.

Such a request should be written with the understanding that it will be reviewed and responded to in keeping with the investigative requirements for contractors, cited in Handbook 6, chapter 2.

#### G. Water Hazards

The computer room has no drainage system to accommodate the overhead sprinkler system. In addition, wiring for the computer and the air conditioning units rests directly on the true floor and is covered by raised flooring. Any appreciable accumulation of water poses a potential safety hazard due to electrical shock and risks equipment damage due to electrical shortages.

Given (1) the elevation of the false floor (approximately 9"), (2) the amount of wiring involved, and (3) the positioning of electrical boxes directly on the true floor, there appears to be no real advantage, or in some instances, no capability to raise the wiring off the floor.

In the past, undetected water leaks have resulted in telephone outages and destruction of paper supplies. Signs of water leakage are also evident along the exterior windows. We believe water leakage accompanies any significant rainfall. In our opinion, the appearance of the exterior wall indicates that the building management has applied only superficial remedies to leakage problems.

The main water turn off valve for the seventh floor is located behind a metal plate in the last stall of the men's restroom. While its location is generally well known, it is not readily accessible.

Recommendation No. 30

We recommend that the Office of Management Operations forward Data Management's request for water detectors to GSA.

Recommendation No. 31

We recommend that the Safety Officer in the Office of Management Operations consider improving the accessibility of the existing water shut off valve.

Recommendation No. 32

We recommend that the Office of Management Operations request the repair of the leaky exterior windows.

H. Schedule and Control Area

Access to the schedule and control area is through Room 736 off the main corridor or through the unauthorized doorway from Room 737. A counter is positioned immediately inside and to the left of doorway 736. The counter, open on both sides and approximately chest high, is used for pickups and deliveries. At the end of the counter is an opening which provides unrestricted access to the schedule and control area and possible access to the computer room itself.

Recommendation No. 33

Because of (1) the volume of traffic in this area, (2) the need to protect Privacy Act Information, and (3) the need to restrict access to the area, we recommend that Data Management, the Office of Management Operations and AG/SEC continue coordinating their efforts to construct a counter/control point.

I. Offsight Storage

Offsight storage for critical tapes and records is essential for any ADP back-up operation. Agreement has been reached between Data Management and MC/GS to utilize the National Records Center in Suitland Maryland as such a facility.

APPENDIX II  
RECOMMENDATIONS

Recommendation No. 1

We recommend that the Bureau for Program and Management Services:

- review and analyze the Data Management security function to determine adequate staffing and support levels, and
- allocate the resources necessary to meet those requirements.

Recommendation No. 2

In order to raise this visibility, and bring the Agency into line with GAO guidelines, we recommend that the Bureau for Program and Management Services establish, coordinate, and oversee an Agency-wide ADP security group or task force reporting directly to the Bureau's Assistant Administrator.

We suggest that the effectiveness of this security group requires the structured participation of all AID offices which have ADP security responsibilities. Some of these AID offices are: the Office of Data Management (SER/DM), the Office of Management Operations (SER/MO), the Office of Public Affairs (OPA), and the Office of the Auditor General (AG).

Recommendation No. 3

Since system users we interviewed were not aware of the status of AID's ADP security or their security responsibilities, we recommend that:

- The Office of Data Management develop, implement, and utilize written procedures establishing on-going methods for periodically informing system owners and users of their responsibilities for data and program security and recovery.

Recommendation No. 4

The Office of Data Management develop a policy statement on ADP security for distribution to system users and other affected parties. This statement should explain the importance of computer security, the office's security goals, and the policies and procedures it follows to achieve those goals.

Recommendation No. 5

We recommend that the Bureau for Program and Management Services contact and coordinate their activities with the Office of Security (AG/SEC) and Office of the General Counsel (GC) to:

- develop a written definition of contract personnel security responsibilities in the ADP environment, and

- define the status of contract personnel as "representatives" of AID, with authority to act in the Agency's behalf in the absence of direct-hire personnel.

#### Recommendation No. 6

To improve utilization of user identification as an access control, we recommend that Data Management change those identifications periodically, but no less frequently than whenever a Data Management staffperson familiar with a system and its data bases leaves his/her position of responsibility.

#### Recommendation No. 7

Since system users seldom change passwords, Data Management must assume responsibility for their control. We recommend that Data Management:

- change passwords assigned to critical and sensitive applications every 6 months or when someone knowledgeable of the password no longer has need to know.
- change passwords assigned to all other applications every 12 months or when someone knowledgeable of the password no longer has a need to know, and
- require system users to notify Data Management when someone knowledgeable of the password no longer has a need to know.

#### Recommendation No. 8

To improve control over password dissemination, we recommend that Data Management modify either the programs or the communication procedures to prevent visual observation of the passwords on the CRT terminals.

#### Recommendation No. 9

To improve RACF utilization, we recommend that:

- The Bureau for Program and Management Services require that all critical and sensitive applications be protected by using RACF.
- Data Management monitor reports produced by the audit attribute of RACF which show attempted accesses to RACF protected applications; isolate and investigate unauthorized access attempts.

#### Recommendation No. 10

Data Management should control the use of AMASPZAP by establishing written procedures for documenting and justifying each use of AMASPZAP.

#### Recommendation No. 11

We recommend that:

- The Office of Data Management develop and implement written procedures

- to control access to the tape library and track the movement of magnetic tapes, These should include a logging procedure to record all movement of tapes into or out of the library.
- The Office of Data Management review its personnel scheduling procedures to consider the feasibility of providing that at least one AID direct-hire employee is in the computer area during all operating shifts. While on duty, this employee should serve as tape librarian with sole access to and control over the library.

#### Recommendation No. 12

Following an inventory to identify media (magnetic tapes and disks) containing "sensitive" data and programs, the Office of Data Management should develop and implement written procedures to provide special protection for such data. These procedures should include a description of duties and responsibilities of personnel handling such data; color coding of the media containing these data; and a maintenance of up-to-date hard copy authorization list of all individuals (computer personnel as well as system users) allowed to access the data. We recommend that management utilize the official guidelines detailed in Standards Publication 41 in developing these procedures.

#### Recommendation No. 13

We recommend that:

- The Chief, General Services Division of the Office of Management Operations (SER/MO/GS) and the Controller, Office of Financial Management (FM), coordinate their activities and implement established procedures to produce a comprehensive building self protection plan, contained in an up-to-date manual, for the Universal North Building.
- The Office of Data Management identify emergency conditions and procedures which have particular implications for ADP operations, such as protection of equipment during a period of civil commotion or loss of control subsequent to a fire, flood, etc. In order to consolidate instructions, these procedures, some of which have already been published in internal DM memoranda, should be included, possibly as amendments, in the revised Building Self-Protection Manual.

#### Recommendation No. 14

We recommend that:

- Data Management and users develop procedures for identifying and ranking critical data and applications.
- The Office of Data Management develop written instructions to system users detailing their responsibilities in reconstructing data files following damage to or destruction of Data Management records
- The Bureau for Program and Management Services, in conjunction with system

users, develop and implement written procedures detailing action to be taken and fixing responsibilities for back-up operations in the event of temporary or permanent damage to the computer center.

#### Recommendation No. 15

We recommend that:

- The Bureau for Program and Management Services should continue to develop a back-up processing plan following the guidance provided in the National Bureau of Standards' Federal Information Processing Standard Publication No. 31, Section 8.3.

#### Recommendation No. 16

To facilitate recovery operations following an emergency at the central computer facility, we recommend that the Office of Data Management formulate and implement recovery procedures based upon the guidance contained in the National Bureau of Standards Federal Information Processing Standards Publication 31.

#### Recommendation No. 17

Physical security provides the most basic form of ADP protection.  
We recommend that:

- The Assistant Administrator of the Bureau for Program and Management Services, in coordination with the General Services Administration, explore available alternative courses of action and identify efforts to remove all non-AID tenants from the 7th floor of the Universal North Building.

#### Recommendation No. 18

We recommend that the safety officer in the Office of Management Operations coordinate with GSA to insure immediate installation of a fire warning system which can be heard throughout the entire 7th floor.

#### Recommendation No. 19

We recommend that Data Management consider the development of an orientation program for their personnel which would instill an awareness of the need for security, advise them of the security-related procedures to be followed, and cite the appropriate chains of command to discuss security-related problems.

#### Recommendation No. 20

Representatives from Data Management and AG/SEC should continue to coordinate and co-author additional instructions as necessary on procedures for (1) emergency access, (2) patrol procedures, and (3) fire and smoke detector response.

Recommendation No. 21

In conjunction with the AG/SEC proposal to close doorway 737, we recommend that Data Management consider alternative plans for means of entry into 737 which would also incorporate fire safety considerations.

Recommendation No. 22

We recommend that representatives from AG/SEC, SER/MO and Data Management continue to meet with personnel from the Social Security Administration and the Japanese American Friendship Commission for purposes of formulating a written agreement defining acceptable identification access procedures and controls for the 7th floor.

Recommendation No. 23

We recommend that Data Management identify their areas by function/equipment sensitivity and that access to those areas deemed sensitive be controlled by an electronic card reader system and physical barriers.

Recommendation No. 24

We recommend that the Safety Officer in the Office of Management Operations:

- post signs clearly reflecting the placement of fire extinguishers;
- have the fire extinguishers inspected and replenished as needed; and
- relocate the fire extinguisher in the tape library to a more accessible area.

Recommendation No. 25

We recommend that the Safety Officer in the Office of Management Operations schedule training for Data Management employees, contractors and guard force personnel in the use of extinguishers and general fire fighting techniques.

Recommendation No. 26

We recommend that the Safety Officer in the Office of Management Operations request a certified electrician review the emergency shut-down plunger system to determine the feasibility and advantages of an electrical current interruption system, located at a point before the transformer.

Recommendation No. 27

We recommend that the Safety Officer in the Office of Management Operations clearly mark the location of smoke detectors with numbers corresponding to the wall panel.

Recommendation No. 28

We recommend that the Safety Officer in the Office of Management Operations consider requiring the relocation of storage room materials to an area which would minimize the impact of a storage room fire upon computer operations.

Recommendation No. 29

In view of the potential problems surrounding Data Management's need for twenty four hour contractor support and the resulting conflict with existing security regulations, we recommend that Data Management either comply with the regulation or justify and formally request exception to the regulation which requires direct hire oversight of contractors working within AID facilities.

Recommendation No. 30

We recommend that the Office of Management Operations forward Data Management's request for water detectors to GSA.

Recommendation No. 31

We recommend that the Safety Officer in the Office of Management Operations consider improving the accessibility of the existing water shutoff valve.

Recommendation No. 32

We recommend that the Office of Management Operations request the repair of the leaky exterior windows.

Recommendation No. 33

Because of (1) the volume of traffic in this area, (2) the need to protect Privacy Act Information, and (3) the need to restrict access to the area, we recommend that Data Management, the Office of Management Operations and AG/SEC continue coordinating their efforts to construct a counter/control point.