

113493  
75683

BY THE COMPTROLLER GENERAL

~~15693~~

# Report To The Congress

## OF THE UNITED STATES

---

### Most Federal Agencies Have Done Little Planning For ADP Disasters

Automatic data processing (ADP) systems are vulnerable to disasters such as fire, power failure, or vandalism. Such occurrences can create havoc with ADP systems.



113993

Most Federal organizations are extremely dependent on ADP systems to meet their operational responsibilities; many would find it impractical, if not impossible, to function without them.

Federal agencies have done little to develop backup plans to counter possible loss of ADP systems and maintain continuity of operations in a disaster. GAO recommends that the Office of Management and Budget take actions to resolve this problem.



013667

AFMD-81-16

DECEMBER 18, 1980

**Request for copies of GAO reports should be sent to:**

**U.S. General Accounting Office  
Document Handling and Information  
Services Facility  
P.O. Box 6015  
Gaithersburg, Md. 20760**

**Telephone (202) 275-6241**

**The first five copies of individual reports are free of charge. Additional copies of bound audit reports are \$3.25 each. Additional copies of unbound report (i.e., letter reports) and most other publications are \$1.00 each. There will be a 25% discount on all orders for 100 or more copies mailed to a single address. Sales orders must be prepaid on a cash, check, or money order basis. Check should be made out to the "Superintendent of Documents".**



COMPTROLLER GENERAL OF THE UNITED STATES

WASHINGTON, D.C. 20548

B-200966

To the President of the Senate and the  
Speaker of the House of Representatives

Federal agencies are extremely dependent upon automatic data processing systems. Most agencies would find it impractical if not impossible to function without such systems.

This report discusses the lack of effort among many Federal agencies to develop backup plans to maintain reasonable continuity of data processing support when normal automatic data processing operations are disrupted.

We are sending copies of this report to the Director of the Office of Management and Budget, the Secretary of Commerce, and the Administrator of General Services.

A handwritten signature in cursive script, reading "James A. Heath".

Comptroller General  
of the United States



D I G E S T

Most Federal agencies rely heavily on automatic data processing (ADP) systems in carrying out their programs; however, such systems are vulnerable to disasters such as floods, fires, earthquakes, or terrorist attacks. Extended loss of the ADP systems that support programs such as Social Security, Medicaid, welfare, pensions, or payrolls could create financial chaos for the programs' recipients.

Federal agencies are required to establish ADP backup plans for maintaining continuity of operations in the event of a disaster. Policy and responsibility for the development and implementation of ADP backup plans by Federal departments and agencies are addressed in OMB Circular A-71, Transmittal Memorandum No. 1, dated July 27, 1978, "Security of Federal automated information systems." (See app. I.)

The memorandum also requires (1) the Department of Commerce to develop and issue ADP security standards and guidelines, to include backup planning, and (2) the General Services Administration to issue policies and regulations consistent with the standards and guidelines issued by Commerce. Recently, the General Services Administration published an amendment to the Federal Procurement Management Regulations which is more definitive in regard to ADP backup planning.

GAO found not only a lack of understanding in the Federal Government of the importance of ADP backup planning, but also that agency top management has not fulfilled its responsibility for implementing Office of Management and Budget requirements for such plans. Of 55 activities reviewed, GAO did not find a single ADP backup plan which it considers adequate. Many activities have only written letters of agreement, which, in GAO's opinion, are not sufficient. (See p. 6.)

An adequate ADP backup plan, with cost-effective options, should reduce the effects of a disaster by providing smooth, rapid restoration of an activity's critical operations until a lost ADP system can be permanently replaced or recovered.

#### AGENCY BACKUP AGREEMENTS-- DEFICIENT AND WITHOUT GUARANTEES

Many agencies, both Government and commercial, appear to provide ADP backup capability to each other through mutual written letters of agreement.

GAO found that such agreements contain many deficiencies--(1) agreements are not always current, (2) fulfilling agreements puts the agency providing the backup in a contingency mode (both parties in an emergency situation), (3) the ADP backup capability is not periodically tested to ensure compatibility of systems, (4) most agreements contain only a single option, and (5) most important, agreements contain no guarantee that the backup equipment will be made available in the event of need.

#### ADDITIONAL BACKUP PROBLEMS WHEN OPERATING SYSTEMS ARE MODIFIED

In some cases agencies have modified vendor-supplied computer operating systems to improve efficiency. GAO has previously advised agencies that this step should be taken only after it is definitely proved that modification is cost effective. If operating systems have been modified, additional backup problems can be encountered. (See p. 8.)

#### IMPORTANCE OF ADP BACKUP PLANNING NEEDS EMPHASIS

Strong leadership is needed to emphasize the importance of ADP backup planning and its role in reducing the risk that loss of ADP capability in an emergency could keep agencies from meeting their responsibilities. OMB's actions have not met the need for strong leadership.

OMB relies on reviews of budgets, plans, and management programs to ensure agency compliance with policies and guidance, but such reviews have not led to agency compliance with established ADP policy.

### CONCLUSIONS

Federal agencies have failed to practice effective risk management. They have not developed adequate ADP backup plans to minimize disruption of their ADP systems and maintain continuity of operations in an emergency.

GAO believes that written letters of agreement for ADP backup are not adequate insurance. A well developed ADP backup plan with cost-effective options should provide for definite continuity of critical operations should normal ADP systems fail.

OMB, in GAO's opinion, has not enforced agency compliance with Circular A-71, Transmittal Memorandum No. 1. OMB reviews of ADP budgets, plans, and management programs have not, to date, ensured compliance with this directive and probably never will.

GAO believes that risk analysis and ADP backup planning require more emphasis and visibility to signify their importance. Top management awareness and involvement are needed to achieve good backup planning. Backup plans should be the topic of discussion for high level ADP executive management committee meetings. Top management has not fulfilled its responsibility to implement OMB Circular A-71, Transmittal Memorandum No. 1.

### RECOMMENDATIONS

Top management within Federal departments and agencies has not met its responsibility for implementing Government policy regarding ADP backup planning. Therefore, the Director of the Office of Management and Budget should:

--Establish a mandatory requirement for each Federal department and agency to

organize an ADP executive committee, with membership comprising top management, to enhance management's involvement in ADP policy and responsibilities, as directed by Federal regulations. This committee should report its activities to OMB before OMB approves the department's or agency's fiscal budget.

- Reaffirm that Federal agencies should test their ADP backup plans periodically to ensure continuity of data processing support in an emergency.
- Request that Inspector General or internal audit groups within each Federal agency evaluate ADP backup plans, review tests and test results in accordance with OMB's criteria, and report their evaluation to the ADP executive committee.
- Ensure that the Department of Commerce develops standards for ADP backup plans.
- Issue policy cautioning against modifying operating system software because of the increased difficulties such modifications cause, particularly in the area of backup.

#### AGENCY COMMENTS

Official comments obtained from the Office of Management and Budget indicated general agreement with most of GAO's findings. OMB expects its planned additional life cycle review of agency information needs to assist OMB in monitoring agency compliance with policies. GAO believes more is required. (See p. 12.)



C o n t e n t s

	<u>Page</u>
DIGEST	i
CHAPTER	
1	INTRODUCTION 1
	Risk management--countermeasure to cope with disaster 1
	Importance of ADP backup planning 2
	What should the ADP backup plan contain? 2
	Federal policy and guidelines for ADP backup planning 3
	Objectives, scope, and methodology 4
2	LACK OF EMPHASIS ON DEVELOPING ADEQUATE ADP BACKUP PLANS 5
	Most agencies have not complied with OMB Circular A-71, TM No. 1 5
	Federal agencies put less importance on ADP backup than do commercial firms 6
	Letters of agreement are not adequate as ADP backup plans 6
	A well developed plan includes cost-effective options 7
	Modified operating systems are an additional problem for backup 8
	ADP backup services are now available commercially 9
	More emphasis is needed on ADP backup planning 10
3	CONCLUSIONS AND RECOMMENDATIONS 11
	Conclusions 11
	Recommendations 12
	Agency comments and our evaluation 12
APPENDIX I	OMB Circular A-71, TM No. 1, "Security of Federal automated information systems" 14

ABBREVIATIONS

ADP	automatic data processing
GAO	General Accounting Office
GSA	General Services Administration
OMB	Office of Management and Budget

## GLOSSARY

Application program	A set of instructions (called program statements or code) to do a specific job, such as payroll computation, inventory control, and accounting. It is also called application software.
Central processing unit	A unit of a computer that includes circuits controlling the interpretation and execution of instructions.
Hardware	The physical equipment of a computer system; e.g., mechanical, magnetic, electrical, or electronic devices; contrasts with software.
Online processing	Pertains to fast response computer processing. It obtains data from an activity or a process; performs computations; and returns a response rapidly enough to control, direct, or influence the outcome of the activity or process.
Operating system	A group of computer programs that monitors and controls the operation of a computer system while the application programs are running.
Software	A set of computer programs, procedures, and associated documentation concerned with operating a data processing system. Three categories of software are (1) application software, (2) operating system software, and (3) utility software.

## CHAPTER 1

### INTRODUCTION

An automatic data processing (ADP) system is a combination of many assets--primarily hardware, software, and personnel. Federal and some State government agencies and private industry firms are extremely dependent upon ADP systems and would find it impractical, if not almost impossible, to function without them. Any temporary or extended loss to any portion of these ADP assets could have tremendous impact on an agency's financial and economic stability.

ADP systems are vulnerable to disasters caused by power failures, floods, fires, earthquakes, disgruntled employees, vandalism, or even terrorist attacks. During the past few years, more than a dozen ADP installations in Europe have been victims of terrorist attacks. Recent disasters that created havoc to ADP systems in the Federal Government include (1) a fire in the data processing center of the Naval Supply Center, Charleston, S. C., and (2) extensive water damage from a faulty sprinkler system in the main computer room at the Bureau of the Census.

ADP system vulnerability to disasters was demonstrated during the 1977 power blackout in New York City. Such power outages can have widespread effects. For example:

- An airline reservation system manager indicated that it costs the airline over \$300,000 through lost reservations each time their ADP system "goes down." 1/
- Air traffic controllers at the major New York airports state that when the ADP system used to control air traffic is down, there are a number of aircraft "near misses."
- A tractor manufacturer said that each ADP system outage costs his firm at least \$50,000 in lost orders for parts.

### RISK MANAGEMENT--COUNTERMEASURE TO COPE WITH DISASTER

Risk management is a method of identifying potential disasters that may cause temporary or extended loss to an ADP

---

1/"Goes down" or "is down" are synonymous terms meaning an ADP system has lost power and is inoperable.

system, and of developing and implementing cost-effective countermeasures to cope with these disasters. ADP backup planning is one aspect of risk management, aimed at reducing the consequences of a disaster that may occur. For the purpose of this report we consider ADP backup plans synonymous with contingency, recovery, or disaster plans.

#### IMPORTANCE OF ADP BACKUP PLANNING

An ADP backup plan is an attempt to reduce the effects of a disaster by providing smooth, rapid restoration of an agency's critical operations until the lost ADP system can be recovered or restored. Loss of an ADP system could have serious repercussions. Federal Government agencies are extremely dependent upon ADP to meet their mission responsibilities, which include administering and maintaining such Federal programs as Social Security, Medicaid, welfare, pensions, or payrolls. A great number of citizens are totally dependent upon the financial security these programs provide. For example, one in six Americans--about 39 million--depends on monthly checks from the Social Security Administration. Extended loss of the ADP systems that support these Federal programs may cause serious financial problems for the programs' recipients.

It is difficult to quantify the total impact of any single ADP system loss. A few days without ADP support might have only minimal effect--or it could cost the Government millions. ADP loss over an extended period, however, could conceivably cause such damage to an agency that it would have great difficulty returning to its normal operation. An adequate ADP backup plan should preclude this possibility.

#### WHAT SHOULD THE ADP BACKUP PLAN CONTAIN?

No ADP backup plan will replace a normal operating environment. The plan's prime purpose is to temporarily counter any disaster that might cause extended loss of an ADP system. We believe the plan should not be restricted to any single disaster; it should be designed to adapt to almost any situation, and the expense should be commensurate with the risk and magnitude of loss.

An effective ADP backup plan is only as good as the options it provides to an agency to continue critical operations in the event of ADP system loss. In our opinion, the plan should include more than one option to be expedient, and only those options that are cost effective should be considered.

It is essential for an agency to conduct periodic testing of the option(s) it has chosen to determine the continuing

effectiveness of its ADP backup plan. Operational requirements may change; therefore, an agency must keep up to date on (1) the continuing availability of the ADP backup capability and (2) hardware and software compatibility. Creation of a sound ADP backup plan requires a lot of time and money. Top management must be involved to approve and budget for the numerous meetings and extensive planning required, and the periodic testing which we believe is essential.

FEDERAL POLICY AND GUIDELINES  
FOR ADP BACKUP PLANNING

Federal policy for ADP backup planning is addressed in Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, dated July 27, 1978, "Security of Federal automated information systems." It requires the heads of Federal departments and agencies to ensure that appropriate ADP backup plans are developed and maintained to provide reasonable continuity of data processing support when normal ADP operations are disrupted. We did not review the other issues addressed in the memorandum.

The memorandum also requires (1) the Department of Commerce to develop and issue ADP security standards and guidelines, to include ADP backup planning, and (2) the General Services Administration (GSA) to issue policies and regulations consistent with the standards and guidelines established by Commerce. Federal Information Processing Standards Publication (FIPS-PUB) 31, issued by the Department of Commerce, contains guidelines for developing ADP backup plans.

Since we completed our review, GSA has published an amendment 1/ which adds a new subpart to Federal Procurement Management Regulation 101-35 and revises Subpart 101-36.7. This addition and revision is somewhat more definitive in regard to ADP backup planning than OMB Circular A-71, Transmittal Memorandum No. 1. It states, for example, that

- arrangements should be made to use a backup facility to operate the essential systems in the event of a total failure;
- recovery procedures should be established to permit rapid restoration of the ADP facility following physical destruction, major damage, or loss of data; and

---

1/F-42, Aug. 11, 1980.

--backup plans should be modified as changes in the ADP facility workload dictate.

If the Federal agencies follow GSA's guidance for ADP backup planning, it will help in maintaining the continuity of ADP operations in an emergency. However, we are concerned about whether Federal agencies will comply with this amendment to the procurement regulations since, in the past, they have not complied with the ADP backup requirements of Transmittal Memorandum No. 1.

#### OBJECTIVES, SCOPE, AND METHODOLOGY

Because ADP systems are costly and have become inseparable from the operation of many Federal programs, the Congress has considerable interest in the monitoring of ADP management by Federal agencies.

Accordingly, our objectives were to determine whether

- Federal agencies have established ADP backup plans for continuity of operations in accordance with OMB Circular A-71, Transmittal Memorandum No. 1, and
- ADP backup plans which have been established are (1) technically and operationally feasible, and (2) updated and tested periodically to ensure reliability.

We reviewed data from 55 activities within the Departments of Agriculture, Commerce, Defense, Justice, Labor, and Treasury. We also visited the Administrative Office of the U.S. Courts, the Comptroller of the Currency, the Federal Reserve Banks of Philadelphia and Richmond, the General Services Administration, and the Office of Management and Budget.

To make a comparative analysis between the Federal Government and the private sector regarding ADP backup planning, we visited 17 firms representing seven major industries--transportation, manufacturing, life and medical insurance, utilities, food services, and banking. We also visited five State governments and two city governments.

We had discussions regarding ADP backup planning with top management at each of the organizations we visited. We reviewed OMB circulars, National Bureau of Standards publications, and agency regulations and procedures. We also talked with representatives of the computer industry who market ADP backup, and researched computer industry trade journals and technical documents.

## CHAPTER 2

### LACK OF EMPHASIS ON DEVELOPING

#### ADEQUATE ADP BACKUP PLANS

We found that, for the most part, the heads of departments and agencies have not met their responsibility for implementing backup planning as required by OMB Circular A-71, Transmittal Memorandum No. 1; nor are they aware of the importance of establishing policies and procedures to ensure that appropriate ADP backup plans are developed and maintained.

#### MOST AGENCIES HAVE NOT COMPLIED WITH OMB CIRCULAR A-71, TM No. 1

In the 55 Federal activities we reviewed, we did not find a single agency ADP backup plan which we consider adequate. Many agencies consider a letter of agreement with another agency to be sufficient ADP backup, but as discussed below, we consider such arrangements inadequate. The following chart summarizes our findings in these agencies.

<u>Number of activities</u>	<u>Backup capability</u>	<u>Comments</u>
31	No ADP backup plan developed	These activities have not complied with OMB Circular A-71, Transmittal Memorandum No. 1, in any form.
8	Oral agreement with another activity	In our opinion these activities have also not complied with TM No. 1 because such an agreement does not constitute adequate backup by any definition.
14	Written letter of agreement with another activity	We believe most of these also do not provide adequate backup for reasons explained in detail on page 6.
2	Classified contingency plans (Defense Department)	These plans are directed toward any (war) emergency, not necessarily ADP. Since they are classified, they have limited accessibility for personnel operating and maintaining general purpose ADP systems. Therefore, we believe such plans do not comply with the intent of OMB Circular A-71, TM No. 1.

FEDERAL AGENCIES PUT LESS IMPORTANCE  
ON ADP BACKUP THAN DO COMMERCIAL FIRMS

Commercial vendors who believe ADP backup is important are attempting to market backup services to Federal agencies. The vendors indicated that most of the Federal agencies they approached have not budgeted funds to either develop and test ADP backup plans or to implement Transmittal Memorandum No. 1. Some commercial corporations which are highly dependent on ADP have recognized the importance of ADP backup. Numerous such corporations have contracted with organizations which specialize in providing ADP backup and recovery services to cover their ADP disaster risks. We are also aware of commercial firms which test their backup plans with surprise simulated catastrophes.

Although the probability of losing a given ADP system as a result of disaster may be remote, Federal agencies cannot afford to ignore the possible effects of such disasters. Adequate ADP backup planning is the advance preparation that should reduce the effects of loss of an ADP system in the event of disaster. Many Federal agencies provide for some ADP backup capability through written letters of agreement with another agency.

LETTERS OF AGREEMENT ARE  
NOT ADEQUATE AS ADP BACKUP PLANS

Written letters of agreement between agencies--promised sharing of processing time to provide ADP backup capability in an emergency--are very popular throughout the Federal Government. Of the activities we reviewed some had written agreements and others had oral agreements which they consider to be adequate ADP backup plans. We do not consider such agreements acceptable to meet the requirement for an appropriate ADP backup plan.

Written letters of agreement may provide temporary comfort to the parties involved, but we found that they can contain serious deficiencies. For example, agreements automatically put the agency providing the equipment for backup in a contingency environment 1/ of its own in event of disaster. Also, there is no firm guarantee that the facility which has agreed by letter to provide ADP backup capability will in fact make its equipment available for the specified periods.

---

1/Lessens the ability of the loaning agency to meet its own needs.



In our opinion, such paper agreements are not real insurance. In addition to the possible deficiencies we have described, it is not uncommon to find equipment compatibility deficiencies in the agreements because they are frequently not kept current or tested periodically with the backup facility.

As the chart on page 5 indicates, 14 Federal activities we reviewed had letters of agreement. These agreements constituted the activity's entire backup plan. Ten of these agreements were over a year old. Only two of the agreements had been tested within the past year. There is therefore no assurance that the backup equipment is still compatible. Some officials stated that periodic testing of the plan was not conducted due to lack of funds or lack of availability of the backup computer.

The Maritime Administration has recently developed and tested a detailed reciprocal letter of agreement for ADP backup with the Smithsonian Institution. While this agreement is not what we consider an ideal ADP backup plan, it might work. Except for the Maritime Administration-Smithsonian agreement, we found no backup agreement that had even identified the agency's critical software applications and assigned priorities to their processing.

Oral ADP backup agreements, which we encountered at eight activities, do not constitute adequate ADP backup plans by any definition.

A WELL DEVELOPED PLAN INCLUDES  
COST-EFFECTIVE OPTIONS

While a written letter of agreement to provide ADP backup capability is of little value alone, a well developed ADP backup plan with cost-effective options may include such a letter as one of the options. Possible options might include, as appropriate for individual circumstances,

- a letter of agreement which relies on another organization with nearly identical ADP equipment agreeing to provide specific amounts of processing time in the event of disaster;
- backup files (program and data) at external storage sites, with guaranteed access to compatible computer equipment;
- standby arrangements for renting processing time or facilities space from commercial vendors who specialize in ADP backup and recovery services;

- a "recovery operation center" (a leased, fully engineered facility, complete except for the computer);
- a shared, fully equipped data processing center for backup, controlled and owned by the participating agencies;
- a multilateral aid agreement involving five to ten agencies who agree to provide a certain amount of ADP capability to the member agency whose operation is disrupted by disaster;
- a redundant ADP system maintained for backup; and
- a plan for reverting to manual operation.

MODIFIED OPERATING SYSTEMS ARE AN  
ADDITIONAL PROBLEM FOR BACKUP

Some agencies will find it difficult to obtain ADP backup capability because they have modified the vendor-supplied operating system software at their installation. Such modification is usually done to obtain higher levels of efficiency. In our June 3, 1974, report to the Congress, 1/ we stated that vendor-supplied operating systems generally should not be modified because:

- Operating system software is usually very complex. Modifications are extremely costly and require qualified experts and considerable computer resources.
- Agencies who modify vendor-supplied operating systems cannot take advantage of new features in computer technology as they become available because they would have to repeatedly modify each new version of the vendor-supplied operating system, thereby incurring substantial and repeated costs.

When an operating system is modified, it is extremely difficult to obtain ADP backup even if comparable computer equipment is available. Operating systems control the processing of application programs--which are instructions to do a specific job such as payroll or accounting. Every modern computer has a vendor-supplied operating system, and their operating characteristics vary among the different vendors.

---

1/"Tools and Techniques For Improving the Efficiency of Federal Automatic Data Processing Operations" (B-115369).

Application programs can be processed without modification only under the operating system for which they were designed.

To provide backup under these circumstances, the agency which provides the backup would have to cease its operations because it is not possible to intermix applications from both agencies on the backup machine. The loaning agency must then load the modified operating system and dedicate its entire computer to processing the workload of the agency requiring backup. Reciprocal backup agreements require that both agencies have comparable computer equipment and compatible operating systems.

Agencies which provide ADP backup to another agency generally have extra processing capacity on their equipment and can, in a reduced state, process not only their own applications but also the applications of the agency requiring backup, providing the operating system is common to both agencies.

It is very doubtful that any agency in the Federal Government would ever be in a position to stop all of its operations and dedicate its computer to another agency. Thus, agencies which modify their operating systems will have a difficult time trying to obtain emergency backup from another agency. Obtaining backup from a commercial source will probably be the only alternative, and this can be very expensive.

The Census Bureau, for example, had modified its UNIVAC computer operating system and had built special programs to process its input and output applications. On August 8, 1979, when Census experienced flooding in its ADP facility, all of its computers suffered water damage. No other Federal or commercial center could provide ready ADP backup without dedicating their entire computer to Census. Consequently, in order to process their high priority applications, Census had to acquire dedicated computer time commercially until its own computer equipment was restored. The cost of leasing and operating this equipment was estimated at more than \$1.5 million.

We believe that a vendor-supplied operating system should not be modified unless it is definitely proved that the modification is cost effective. Furthermore, when a vendor-supplied operating system is modified, the impact of the modification on backup capabilities should be carefully considered.

ADP BACKUP SERVICES ARE NOW  
AVAILABLE COMMERCIALY

Because of the growing demand for ADP backup capability, vendors are now providing such services. Commercial vendors specializing in ADP backup services are available, at a price,

to supply guaranteed ADP service or facility space or both to any customer agency who experiences ADP downtime for an extended period. Such contractual arrangements for ADP backup must be entered into before any disaster strikes. Any agency which may require ADP backup, can, if it is so arranged and paid for in advance, be on-line at one of these commercial backup facilities within 4 hours. Annual premiums vary in cost, depending upon the type of ADP backup service required.

The Federal Reserve Bank of Philadelphia recently signed a contract for emergency ADP backup service. Bank officials indicated that the cost of the service was trivial compared to the potential dollar loss that would be incurred should they not be able to process their money transfers--more than \$7.5 billion a day--over an extended period of time.

MORE EMPHASIS IS NEEDED ON  
ADP BACKUP PLANNING

Strong leadership is needed to emphasize the importance of ADP backup planning and its role in reducing the risk that agencies might be unable to meet their assigned responsibilities in an emergency.

OMB issues policy and the Department of Commerce and GSA issue standards and guidance to Federal agencies concerning the management and use of ADP equipment. However, over the years Federal agencies have sometimes shown a reluctance to follow certain policy and guidance. ADP backup planning also appears to fall into this category.

Simply issuing regulations is not sufficient to ensure that agency responsibilities are met. OMB relies on review of budgets, plans, and management programs to ensure compliance with policies and guidance. In our opinion, such reviews have not led to agency compliance with established policy for ADP backup planning. We are aware of no agency that has developed what we consider to be an adequate ADP backup plan.

## CHAPTER 3

### CONCLUSIONS AND RECOMMENDATIONS

#### CONCLUSIONS

ADP systems are vulnerable to many types of disasters. Whether accidental or deliberate, such disasters can and do happen. In the Federal Government, where the dependency on ADP systems is so great, very few agencies can afford the loss of their ADP system through such a disaster.

We believe that a well developed ADP backup plan with cost-effective options is a method of risk management that would provide reasonable ADP support for continuity of operations and thereby reduce the consequences of a disaster. While the newly published GSA regulation is somewhat more definitive regarding backup than OMB Circular A-71, Transmittal Memorandum No. 1, we do not believe it is sufficiently detailed to serve as adequate guidance for agencies. Still more definitive material is needed.

Of the Federal activities we reviewed, none has developed what we consider to be an adequate ADP backup plan with cost-effective options. Therefore, we believe agencies are not prepared to cope with the loss of their ADP systems in an emergency.

Agencies in the Federal Government rely almost exclusively on written or oral reciprocal agreements for ADP backup capability. In our opinion, such agreements are of little value because they contain no guarantee that the reciprocating agency's ADP equipment will be available if needed.

OMB has not enforced conformance to its policy on ADP backup planning by agencies. In our view, OMB reviews of ADP budgets, plans, and management programs have not, to date, assured compliance with OMB Circular A-71, Transmittal Memorandum No. 1, and probably never will.

We believe risk management and ADP backup planning need more top management awareness and involvement because of their importance. These issues should be discussed in high level agency ADP executive management committee meetings. ADP backup planning costs money, and top management must be involved to be aware of the need to budget for it.

We further believe that operating system software should not be modified unless there are definite indications that the modification is cost effective.

## RECOMMENDATIONS

Top management within Federal departments and agencies has not met its responsibility for implementing Government policy regarding ADP backup planning. Therefore, the Director of the Office of Management and Budget should:

- Establish a mandatory requirement for each Federal department and agency to organize an ADP executive committee, with membership comprising top management, to enhance management's involvement in ADP policy and responsibilities, as directed by Federal regulations. This committee should report its activities to OMB before OMB approves the department's or agency's fiscal budget.
- Reaffirm that Federal agencies should test their ADP backup plans periodically to ensure continuity of data processing support in an emergency.
- Request that Inspector General or internal audit groups within each Federal agency evaluate ADP backup plans, review tests and test results in accordance with OMB's criteria, and report their evaluation to the ADP executive committee.
- Ensure that the Department of Commerce develops standards for ADP backup plans.
- Issue policy cautioning against modifying operating system software because of the increased difficulties such modifications cause, particularly in the area of backup.

## AGENCY COMMENTS AND OUR EVALUATION

In commenting on this report, the Office of Management and Budget generally agreed with most of our findings.

Although OMB agreed that ADP backup planning should get more emphasis, it believes that such plans are only a small part of its total responsibility under OMB Circular A-71, Transmittal Memorandum No. 1, and that OMB attention must focus on the entire memorandum, not just parts of it. In our view, ADP backup planning is a discrete area and should receive special emphasis because of the potential problems involved.

OMB agrees with our view that a letter of agreement alone does not constitute an adequate ADP backup plan. An effective backup plan needs more than one option.

OMB stated that its review of budgets, plans, and management programs is the best method available to monitor agency compliance with ADP policies and guidance. As a result of its recent reorganization, OMB now plans to add a review of the life cycle of an agency's information needs from its regulatory requirements through collection and internal processing rather than review each of these activities separately, as it has been doing. According to OMB this life cycle review is expected to assist OMB in monitoring ADP programs by identifying the information being collected by the agency. We still doubt that this approach by OMB is sufficient, and we believe that the additional action recommended in this report is necessary to resolve the problem.



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

July 27, 1978

CIRCULAR NO. A-71  
Transmittal Memorandum No. 1

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Security of Federal automated information systems

1. Purpose. This Transmittal Memorandum to OMB Circular No. A-71 dated March 6, 1965 promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies. More specifically, It:

a. Defines the division of responsibility for computer security between line operating agencies and the Department of Commerce, the General Services Administration, and the Civil Service Commission.

b. Establishes requirements for the development of management controls to safeguard personal, proprietary and other sensitive data in automated systems.

c. Establishes a requirement for agencies to implement a computer security program and defines a minimum set of controls to be incorporated into each agency computer security program.

d. Requires the Department of Commerce to develop and issue computer security standards and guidelines.

e. Requires the General Services Administration to issue policies and regulations for the physical security of computer rooms consistent with standards and guidelines issued by the Department of Commerce; assure that agency procurement requests for automated data processing equipment, software, and related services include security requirements; and assure that all procurements made by GSA meet the security requirements established by the user agency.

f. Requires the Civil Service Commission to establish personnel security policies for Federal personnel associated



with the design, operation or maintenance of Federal computer systems, or having access to data in Federal computer systems.

2. Background. Increasing use of computer and communications technology to improve the effectiveness of governmental programs has introduced a variety of new management problems. Many public concerns have been raised in regard to the risks associated with automated processing of personal, proprietary or other sensitive data. Problems have been encountered in the misuse of computer and communications technology to perpetrate crime. In other cases, inadequate administrative practices along with poorly designed computer systems have resulted in improper payments, unnecessary purchases or other improper actions. The policies and responsibilities for computer security established by this Transmittal Memorandum supplement policies currently contained in OMB Circular No. A-71.

3. Definitions. The following definitions apply for the purposes of this memorandum:

a. "Automated decisionmaking systems" are computer applications which issue checks, requisition supplies or perform similar functions based on programmed criteria, with little human intervention.

b. "Contingency plans" are plans for emergency response, back-up operations and post-disaster recovery.

c. "Security specifications" are a detailed description of the safeguards required to protect a sensitive computer application.

d. "Sensitive application" is a computer application which requires a degree of protection because it processes sensitive data or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application (e.g., automated decisionmaking systems).

e. "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).

4. Responsibility of the heads of executive agencies. The head of each executive branch department and agency is

responsible 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 not subject to national security regulations, as well as national security data. 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. The agency's computer security program shall be consistent with all Federal policies, procedures and standards issued by the Office of Management and Budget, the General Services Administration, the Department of Commerce, and the Civil Service Commission. In consideration of problems which have been identified in relation to existing practices, each agency's computer security program shall at a minimum:

a. Assign responsibility for the security of each computer installation operated by the agency, including installations operated directly by or on behalf of the agency (e.g., government-owned contractor operated facilities), to a management official knowledgeable in data processing and security matters.

b. Establish personnel security policies for screening all individuals participating in the design, operation or maintenance of Federal computer systems or having access to data in Federal computer systems. The level of screening required by these policies should vary from minimal checks to full background investigations commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies should be established for government and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Civil Service Commission.

c. Establish a management control process to assure that appropriate administrative, physical and technical safeguards are incorporated into all new computer applications and significant modifications to existing computer applications. This control process should evaluate the sensitivity of each application. For sensitive applications, particularly those which will process sensitive data or which will have a high potential for loss,

such as automated decisionmaking systems, specific controls should, at a minimum, include policies and responsibilities for:

(1) Defining and approving security specifications prior to programming the applications or changes. The views and recommendations of the computer user organization, the computer installation and the individual responsible for the security of the computer installation shall be sought and considered prior to the approval of the security specifications for the application.

(2) Conducting and approving design reviews and application systems tests prior to using the systems operationally. The objective of the design reviews should be to ascertain that the proposed design meets the approved security specifications. The objective of the system tests should be to verify that the planned administrative, physical and technical security requirements are operationally adequate prior to the use of the system. The results of the design review and system test shall be fully documented and maintained as a part of the official records of the agency. Upon completion of the system test, an official of the agency shall certify that the system meets the documented and approved system security specifications, meets all applicable Federal policies, regulations and standards, and that the results of the test demonstrate that the security provisions are adequate for the application.

d. Establish an agency program for conducting periodic audits or evaluations and recertifying the adequacy of the security safeguards of each operational sensitive application including those which process personal, proprietary or other sensitive data, or which have a high potential for financial loss, such as automated decisionmaking applications. Audits or evaluations are to be conducted by an organization independent of the user organization and computer facility manager. Recertifications should be fully documented and maintained as a part of the official documents of the agency. Audits or evaluations and recertifications shall be performed at time intervals determined by the agency, commensurate with the sensitivity of information processed and the risk and magnitude of loss or harm that could result from the application operating improperly, but shall be conducted at least every three years.

e. Establish policies and responsibilities to assure that appropriate security requirements are included in

specifications for the acquisition or operation of computer facilities, equipment, software packages, or related services, whether procured by the agency or by the General Services Administration. These requirements shall be reviewed and approved by the management official assigned responsibility for security of the computer installation to be used. This individual must certify that the security requirements specified are reasonably sufficient for the intended application and that they comply with current Federal computer security policies, procedures, standards and guidelines.

f. Assign responsibility for the conduct of periodic risk analyses for each computer installation operated by the agency, including installations operated directly by or on behalf of the agency. The objective of this risk analysis should be to provide a measure of the relative vulnerabilities at the installation so that security resources can effectively be distributed to minimize the potential loss. A risk analysis shall be performed:

(1) Prior to the approval of design specifications for new computer installations.

(2) Whenever there is a significant change to the physical facility, hardware or software at a computer installation. Agency criteria for defining significant changes shall be commensurate with the sensitivity of the information processed by the installation.

(3) At periodic intervals of time established by the agency, commensurate with the sensitivity of the information processed by the installation, but not to exceed five years, if no risk analysis has been performed during that time.

g. Establish policies and responsibilities to assure that appropriate contingency plans are developed and maintained. The objective of these plans should be to provide reasonable continuity of data processing support should events occur which prevent normal operations. These plans should be reviewed and tested at periodic intervals of time commensurate with the risk and magnitude of loss or harm which could result from disruption of data processing support.

5. Responsibility of the Department of Commerce. The Secretary of Commerce shall develop and issue standards and

guidelines for assuring security of automated information. Each standard shall, at a minimum, identify:

- a. Whether the standard is mandatory or voluntary.
- b. Specific implementation actions which agencies are required to take.
- c. The time at which implementation is required.
- d. A process for monitoring implementation of each standard and evaluating its use.
- e. The procedure for agencies to obtain a waiver to the standard and the conditions or criteria under which it may be granted.

6. Responsibility of the General Services Administration.  
The Administrator of General Services shall:

- a. Issue policies and regulations for the physical security of computer rooms in Federal buildings consistent with standards and guidelines issued by the Department of Commerce.

- b. Assure that agency procurement requests for computers, software packages, and related services include security requirements which have been certified by a responsible agency official. Delegations of procurement authority to agencies by the General Services Administration under mandatory programs, dollar threshold delegations, certification programs or other so-called blanket delegations shall include requirements for agency specifications and agency certification of security requirements. Other delegations of procurement authority shall require specific agency certification of security requirements as a part of the agency request for delegation of procurement authority.

- c. Assure that specifications for computer hardware, software, related services or the construction of computer facilities are consistent with standards and guidelines established by the Secretary of Commerce.

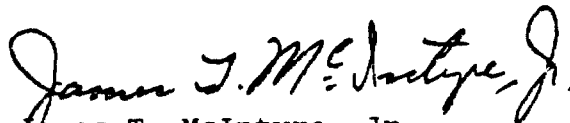
- d. Assure that computer equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by the General Services Administration meet the security requirements established by the user agency and are

consistent with other applicable policies and standards issued by OMB, the Civil Service Commission and the Department of Commerce. Computer equipment, software, or related ADP services acquired by the General Services Administration in anticipation of future agency requirements shall include security safeguards which are consistent with mandatory standards established by the Secretary of Commerce.

7. Responsibility of the Civil Service Commission. The Chairman of the Civil Service Commission shall establish personnel security policies for Federal personnel associated with the design, operation or maintenance of Federal computer systems, or having access to data in Federal computer systems. These policies should emphasize personnel requirements to adequately protect personal, proprietary or other sensitive data as well as other sensitive applications not subject to national security regulations. Requirements for personnel checks imposed by these policies should vary commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused by the individual. The checks may range from merely normal reemployment screening procedures to full background investigations.

8. Reports. Within 60 days of the issuance of this Transmittal Memorandum, the Department of Commerce, General Services Administration and Civil Service Commission shall submit to OMB plans and associated resource estimates for fulfilling the responsibilities specifically assigned in this memorandum. Within 120 days of the issuance of this Transmittal Memorandum, each executive branch department and agency shall submit to OMB plans and associated resource estimates for implementing a security program consistent with the policies specified herein.

9. Inquiries. Questions regarding this memorandum should be addressed to the Information Systems Policy Division (202) 395-4814.

  
James T. McIntyre, Jr.  
Director

**AN EQUAL OPPORTUNITY EMPLOYER**

**UNITED STATES  
GENERAL ACCOUNTING OFFICE  
WASHINGTON, D.C. 20548**

**OFFICIAL BUSINESS  
PENALTY FOR PRIVATE USE, \$300**

**POSTAGE AND FEES PAID  
U. S. GENERAL ACCOUNTING OFFICE**



**THIRD CLASS**

