# NCJRS

This microfiche was produced from documents received for inclusion in the NCJRS data base. Since NCJRS cannot exercise control over the physical condition of the documents submitted, the individual frame quality will vary. The resolution chart on this frame may be used to evaluate the document quality.
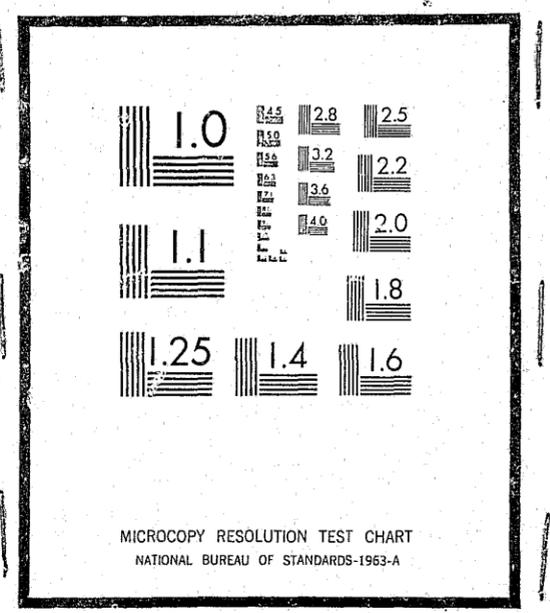
Microfilming procedures used to create this fiche comply with the standards set forth in 41CFR 101-11.504

Points of view or opinions stated in this document are those of the author(s) and do not represent the official position or policies of the U.S. Department of Justice.

U.S. DEPARTMENT OF JUSTICE
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
NATIONAL CRIMINAL JUSTICE REFERENCE SERVICE
WASHINGTON, D.C. 20531

4/12/77
Date filmed

---

*REPORT TO THE CONGRESS*

*BY THE COMPTROLLER GENERAL OF THE UNITED STATES*

## Managers Need To Provide Better Protection For Federal Automatic Data Processing Facilities

Multiagency

Physical security policies and practices employed at Federal data processing installations to prevent losses caused by bombings, fires, floods, frauds, thefts, embezzlements, and human errors need improvement.

GAO recommends that the Office of Management and Budget direct that

--at each Federal computer installation a management official be designated as specifically responsible for automatic data processing physical security and

--he use risk management techniques when determining the protection needed.

NCJRS

NOV 22 1976

...TIONS

FGMSD-76-40    MAY 10, 1976

B-115369

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

This report summarizes our findings about the adequacy
of physical security and risk management policies and prac-
tices employed at Federal data processing installations to
prevent losses caused by bombings, fires, floods, frauds,
thefts, embezzlements, and human errors.

We made our review pursuant to the Budget and Accounting
Act, 1921 (31 U.S.C. 53), and the Accounting and Auditing Act
of 1950 (31 U.S.C. 67).

We are sending copies of this report to the Director,
Office of Management and Budget; the Secretary of Commerce;
and heads of Federal departments and agencies.

Comptroller General
of the United States

# Contents

APPENDIX

## ABBREVIATIONS

ADP     automatic data processing

GAO     General Accounting Office

GSA     General Services Administration

NBS     National Bureau of Standards

OMB     Office of Management and Budget

MANAGERS NEED TO PROVIDE
BETTER PROTECTION FOR
FEDERAL AUTOMATIC DATA
PROCESSING FACILITIES
Multiagency

## D I G E S T

Currently the Federal Government relies on the
services of about 9,000 computers in its day-to-
day operations. The total value of this equip-
ment is many billions.

The value of some of the data which is proc-
essed on these computers, such as social secu-
rity records, is immeasurable. Consequently,
protecting equipment and data from unauthorized
or inadvertent acts of destruction, alteration
or misuse is a matter of inestimable importance.

To illustrate, the National Aeronautics and
Space Administration could not carry forth its
space programs and the Federal Aviation Adminis-
tration could not control aircraft effectively
without computer assistance. Many computers
are used to manage the more than half-billion
transactions processed by the Social Security
Administration and the four billion facts relat-
ing to the national population compiled and
managed by the Bureau of the Census. Many
other agencies could continue to function only
at reduced levels of efficiency and effective-
ness if computers were not used.

Catastrophic losses to Government-sponsored
data processing installations, such as the loss
of human life, irreplaceable data, and equipment,
have occurred. In many of the examples cited,
additional security measures were implemented
subsequent to the loss. (See pp. 7 to 26.)

Information on the physical security measures
employed by 28 Federal data processing facili-
ties led GAO to believe that many Federal
data processing assets and much valuable data
are not protected properly. (See p. 5.)

Tear Sheet. Upon removal, the report
cover date should be noted hereon.

i

FGMSD-76-40

Some managers were not confident that they had the right degree of security for their facility; some have implemented sophisticated physical security measures, and others have operated with minimal security. (See p. 27.)

Less than half of the 28 installations visited had developed and put into operation contingency plans to provide for continuity of operations if a loss occurred. (See p. 22.) The impact from losses at data processing installations which did not have contingency plans could

> --interfere seriously with efficient and economical operations of Government,

> --have an immeasurable impact on individuals and organizations relying on Government data, and

> --result in costly reconstruction efforts.

Managers of Federal data processing centers have been undertaking physical security measures based on experience, subjective judgment, and advice received from managers of other installations. (See p. 27.)

In 1974 the National Bureau of Standards issued guidelines for establishing physical security measures for data processing activities.

The guidelines provide detailed suggestions for making essential security decisions. This includes use of a risk management concept where security measures are related to the value of the data and the equipment; i.e., costly measures would not be taken to protect data or equipment of relatively low value.

The National Bureau of Standards guidelines provide the suggestions needed for a strong security program. However, the guidelines, as issued, are only a reference document and there is no requirement that agencies must use them when determining their security needs. (See p. 30.)

To provide more security over Government automatic data processing operations at a

reasonable cost, GAO recommends that the
Director of the Office of Management and
Budget direct that management officials be
appointed at Federal installations having data
processing systems and that they be assigned
responsibility for automatic data processing
physical security and risk management.  GAO
also recommends that these officials be di-
rected to use the National Bureau of Stand-
ards guidelines when developing physical
security and risk management programs.  (See
p. 34.)

The Office of Management and Budget agreed
that there is a need for a greater awareness
of threats to physical security and said that
this report should serve as a strong reminder
to Federal managers on the importance of
security measures for automatic data processing
facilities.  It questioned, however, the appro-
priateness of directing that a separate offi-
cial be named for automatic data processing
security.  The Office of Management and Budget
believes the agency head should be responsible
for determining both the security measures
needed, as well as how to organize its opera-
tions to insure effective security.

GAO recognizes that an agency head is
responsible for the agency's overall management
and operation and this makes his day-to-day
responsibilities most demanding.  Since data
processing operations are so important to the
well-being of most agencies, GAO believes that
this responsibility should be delegated to a
management official who is knowledgeable in
agency missions, as well as in data processing
and security matters.  (See p. 31.)

# CHAPTER 1

## INTRODUCTION

Computers have become an integral part of the Government process by performing many of the operations and applications that, in the past, were not done at all or were done manually. Some agencies would find it impractical, if not impossible, to accomplish their missions without computers. To illustrate, the National Aeronautics and Space Administration could not carry forth its space programs and the Federal Aviation Administration could not control aircraft effectively without computer assistance. Many computers are used to manage the more than half billion transactions annually, processed by the Social Security Administration and the four billion facts relating to the national population compiled and managed by the Bureau of the Census. Many other agencies could continue to function only at reduced levels of efficiency and effectiveness if computers were not used.

The Federal Government is the largest user of computers. In addition to the cost of acquiring and operating computers, vast sums are expended for

--software programs to make computers run,

--communication links between computer components,

--buildings and associated expenses to house data processing operations, and

--processing and storing data.

It has been estimated that over $10 billion is spent annually to acquire equipment and to operate Federal data processing activities.

Of more importance than the concern over the monetary value of these assets is the centralization and concentration of data in computerized environments which increases the potential for major losses or misuses that could

--affect the successful accomplishment of agency mission and goals,

--have an impact on those who rely on valuable or irreplaceable Government records, or

--harm individuals on whom information is maintained.

1

There is, therefore, a need to protect these assets an co provide for continuity of operations should a catastrophe occur.

## SOME DEFINITIONS

Data processing security is a means of safeguarding hardware, software, data, personnel, and facilities against loss from accidental or intentional disclosure t data, modification of data, destruction of assets, or both. Physical security includes the protection of equipment, personnel, facilities, and data involved with computerized processing; and provides for recovery in case of damage or loss. Such protection is provided by various means, including restrictive access and administrative controls for data processing activities, as well as applying other measures required for protection of structures, equipment and data against accidents, fires, floods, bombings, and other hazards.

Perfect security is generally regarded as unattainable; therefore, the aim of a good physical security system should be to reduce the probability of loss to an acceptable low level at reasonable cost and to insure adequate recovery in case of loss. Many articles and publications have been written lately which say that a good securi program can only be achieved by having high level management responsible for the automatic data processing (ADP) security program and using some type of systematic approach when making physical security decisions.

There are many ways and approaches to help management make ADP security decisions. One approach advocated by experts, which we believe to be a good approach, involves a concept of risk management. This concept is an element of managerial science that is concerned with identification, measurement and control of uncertain events. It

--analyzes the risks involved,

--summarizes risk findings for management use,

.--involves high level management in the decisionmaking process,

--implements the most cost effective security practices to control unacceptable risks, and

--reevaluates periodically the potential impacts from threats to asset values and mission accomplishments

2

and decides on new or existing practices to handle
the risks.

For a full explanation of this concept, see appendix I.

Proper physical security, as discussed in this report,
is a prerequisite to achieving adequate data security and
privacy protection. To have safe and reliable Govern-
ment data, it is necessary to have a good data security
program for protection against accidental or intentional
destruction, disclosure or modification of data in a system.
In a computerized system where large quantities of data can
be centrally accumulated, stored, and integrated with data
from other systems, appropriate administrative, technical
and physical safeguards are more necessary than in a manual
system.

## RESPONSIBILITY FOR SECURITY

Public Law 89-306 (Brooks Act) was passed in October
1965 and provides for the economic and efficient purchase,
lease, maintenance, operation, and utilization of ADP
equipment. The General Services Administration (GSA) is
responsible for the economic and efficient acquisition,
use, and maintenance of ADP equipment; the Office of Manage-
ment and Budget (OMB) is responsible for policy and fiscal
control aspects of ADP management. The law also provides
for the Department of Commerce to be responsible for
developing technical standards and providing technical
advisory services to Federal agencies.

In turn, heads of departments and agencies are authorized
by Public Law 89-554 to prescribe regulations for the custody
and preservation of their records, papers, and property. The
Privacy Act of 1974, Public Law 93-579, requires, among other
things, that each agency maintaining a system of records pro-
vide appropriate safeguards to insure the security of its
data.

## SCOPE OF STUDY

Our study covered Government-wide policies and practices
used for determining physical security requirements at Federal
data processing installations. More specifically, we examined:

--Policies and procedures established by OMB and
GSA regarding automatic data processing systems.

--Security techniques employed at 28 data processing
installations by the Departments of the Army; Navy;

Air Force; Agriculture; Transportation; State; and
Health, Education, and Welfare and the Veterans
Administration.

--Types of data processing security used at selected
Government contractors, universities, private
companies, a bank, and a local government.

--Types of security problems experienced at 23
additional Federal data processing installations.

Major areas of security covered during our visits in-
cluded steps taken by management to guard against threats of
modification or destruction to the physical plant, person-
nel, computer hardware and software, and to the data being
processed or stored by the computerized systems. We de-
veloped and used a questionnaire as an audit guideline for
these visits.

A detailed compilation of data from the questionnaires
is shown in appendix II. This material represents those
areas of automatic data processing security that applied to
each installation visited and that could be quantified for
analyses.

4

# CHAPTER 2

## SECURITY AT FACILITIES VISITED

## WAS INADEQUATE

To obtain information on the effectiveness of procedures employed by Federal agencies, we visited 18 data processing installations within the continental United States and 10 installations overseas and observed the protection procedures for equipment and valuable data.

We found a number of conditions at these 28 installations which led us to believe that physical security was not adequate and that action should be taken to protect against losses. Some of the conditions we found which we believe provided insufficient protection to data processing equipment and data follow.

| Conditions found (note a) | Locations within the continental United States | Locations overseas |
|---|---|---|
| Fire hazards: | | |
| Combustible paper supplies and/ or magnetic tape files were stored in computer rooms which expose systems to losses from fire. | 10 | 4 |
| Computers were in use in areas with only portable fire extinguishers available. | 3 | - |
| Computers were in operation in room with no portable fire extinguishers available. | - | 1 |
| Computers were in use above raised flooring without periodically cleaning below such flooring, which is a fire potential. | 12 | - |
| Computers were in operation in rooms where master electrical power shutdown controls were not easily accessible at exit points. | 2 | 4 |

| Conditions found | Locations within the continental United States | Locations overseas |
|---|---|---|
| Flood hazards: | | |
| Computers were in operation in areas where overhead water or steam pipes (excluding sprinkler systems, existed with inadequate provision for drainage. | 10 | - |
| Computers were used in basements below ground level which exposes systems to potential flooding conditions. | 2 | - |
| Susceptible to sabotage: | | |
| Vendor service personnel were not supervised while on premises. | 7 | - |
| In-house service personnel not controlled while in computer areas. | 5 | - |
| Computer location was possible target for vandals. | 3 | - |
| Susceptible to theft or misuse: | | |
| Remotely accessed computer systems were in operation without software to detect improper or erroneous attempts to use the computers or data files involved. | 3 | 2 |
| Lack of contingency planning: | | |
| Computerized systems were in operation without formal contingency plans to insure continuity of operations if a security event occurred. | 8 | 6 |

a/Details supporting these and other observations relating to the lack of physical security measures are shown in appendix II.

Although the above hazardous conditions existed at sites
visited, the installations had not necessarily experienced
an adverse effect or loss from the lack of good physical
security measures. Weaknesses, such as those noted above,
however, can lead to serious consequences. We supplemented
our visits by contacting 23 other Federal data processing
installations within the continental United States--some of
which we knew have had physical security problems--to
identify impacts or effects from security weaknesses.

Of the 23 installations contacted 9 have experienced
physical damages from conditions, such as attempted sabotage,
fires, and floods, since January 1970. Some of the losses
experienced by these and other installations are shown below
to emphasize the devastating effects fire, flood, and sabo-
tage, can have upon data processing facilities.

FIRE

Fires can cause minimal or catastrophic losses.
The extent of the loss generally depends upon factors such
as size and location of the fire, extent and type of fire
protective devices at an installation, and the type of
contingency plan available if a fire should occur.

A classic example of fire loss is the 1959 fire at the
Pentagon, which destroyed three complete computer systems
valued at $6.5 million. (See picture on p. 8.) The fire
started in a vault containing stored paper and magnetic
tape and spread throughout the computer center. When the
fire occurred employees were unable to reach the switch to
turn off electrical power for the computer systems which
created a hazardous situation for firefighting efforts.

We did not attempt to relate the hazardous fire con-
ditions we found at the 14 locations noted on page 5 to
the hazardous fire condition that caused the Pentagon fire.
However, we do believe that the Pentagon fire clearly
illustrates what could be lost by fire at the 14 locations
which had combustible paper or magnetic tape stored in
computer rooms. Also, if a fire did occur at the 6
locations noted in our study (see p. 5) where master
electrical power shutdown controls were not easily acces-
sible, the employees at the 6 locations, just like the
employees in the Pentagon fire, would be unable to shut off
electrical power for the computer systems.

While no major fire to Government ADP facilities has
occurred lately, commercial installations have not been so
lucky. For example, there was a much publicized commercial
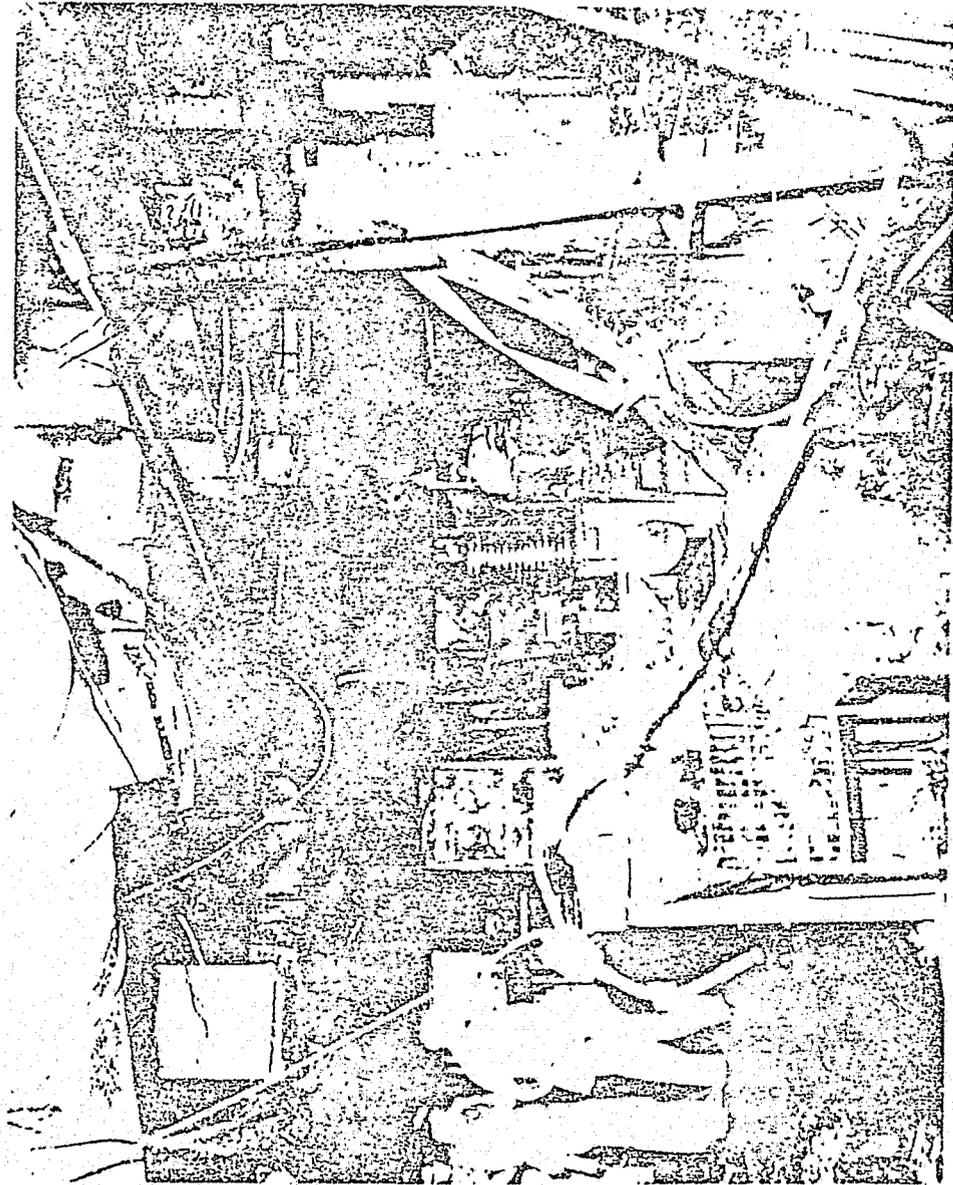
VIEW OF PENTAGON COMPUTER FACILITY DAMAGE AFTER FIRE
(Courtesy of Department of Air Force)

8
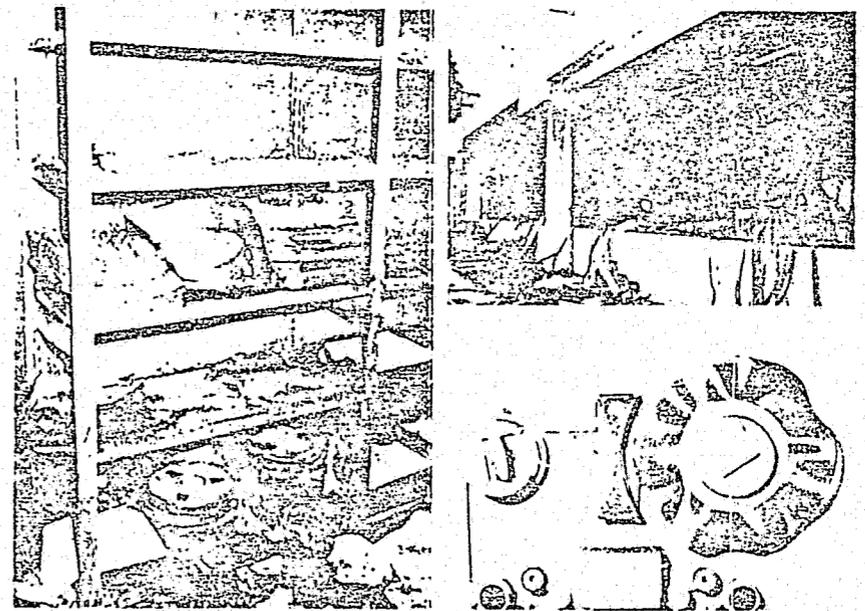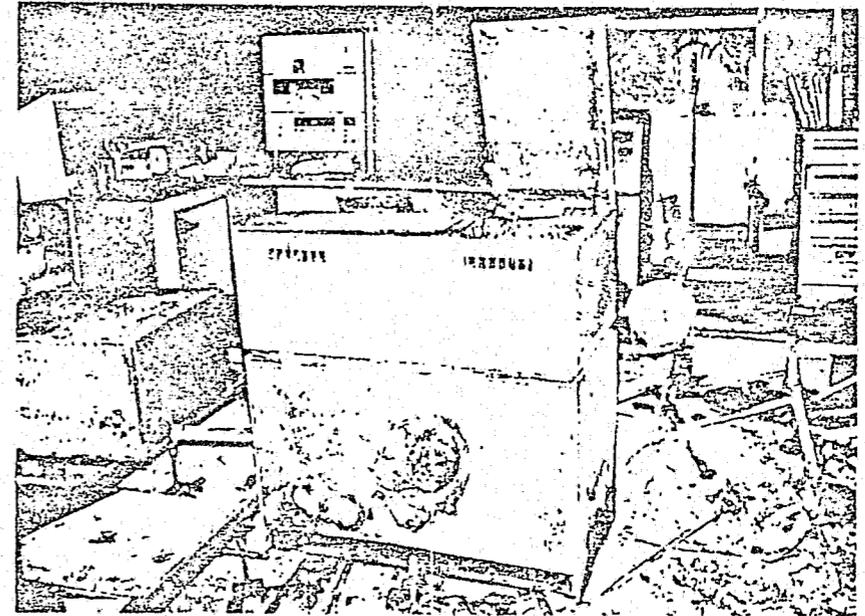
VIEW OF DAMAGE DONE TO COMMERCIAL COMPUTER FACILITY
(Courtesy of International Business Machines Corporation)

9
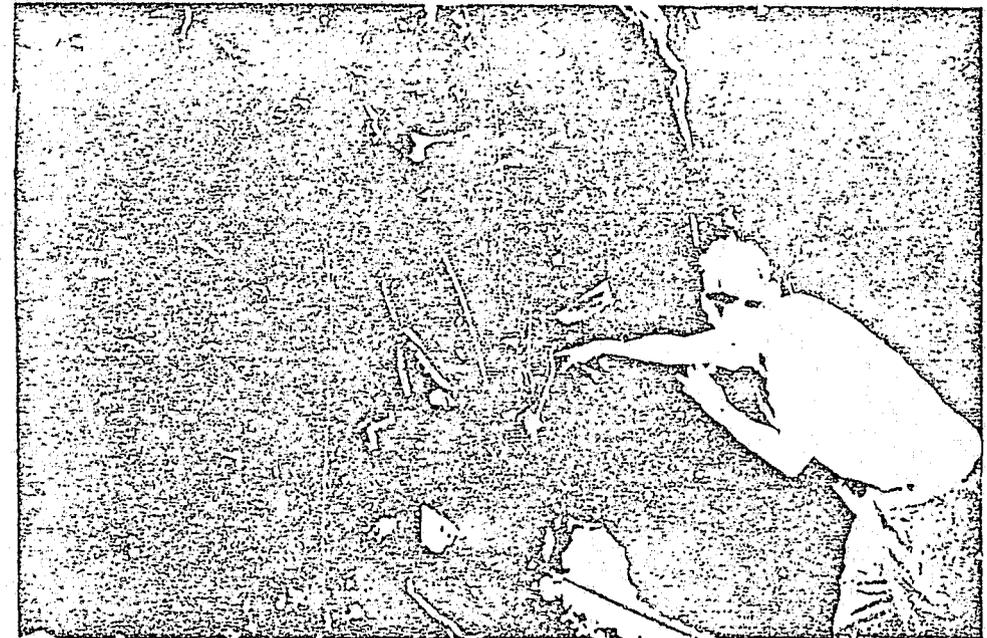
VIEW OF ASHEN RECORDS AND SHELVING
(Courtesy of General Services Administration)
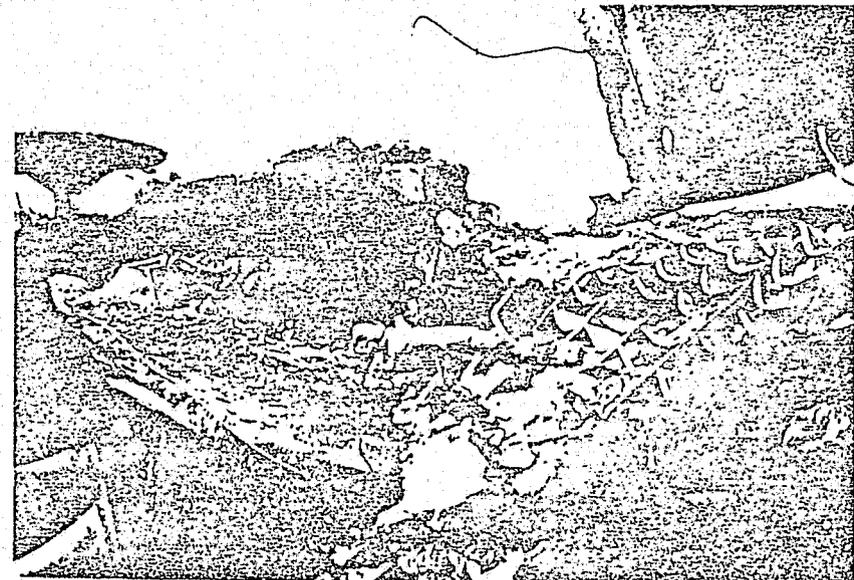


VIEW OF BUILDING CRUSHED BY COLLAPSED ROOF
AFTER ST. LOUIS FIRE
(Courtesy of General Services Administration)

10

fire in 1972 which caused a $1 million loss at International
Business Machines Corporation, Hawthorne, New York. (See
p. 9.)

Another example of a catastrophic loss caused by fire to
a Government facility, although computer records were not
directly involved, was the fire at the Military Personnel
Records Center in St. Louis, Missouri, in July 1973. Sections
of the building housing these records were not equipped with
sprinkler systems, smoke detectors or fire walls. Although
the fire did major damage to paper and not computerized records
it nevertheless illustrates how devastating the loss of ir-
replaceable documents and records can be. Since such records
are being put on computers more and more the problem in-
creasingly becomes a computer security problem. (See p. 10.)

The records center has been the repository for about
52 million records on military personnel actions since 1912.
The sixth floor, where the fire started, contained about
22 million military personnel files or jackets. About
16.8 million of these records were lost.

Painstaking work is necessary to reconstruct the lost
records and some may never be replaced.

Of the 18 locations we visited in the United States, 3
had only portable fire extinguishers available for firefight-
ing protection. Also, one overseas location did not even
have any fire extinguishers available for firefighting
operations. (See p. 5.)

FLOOD

Since water can cause serious damage to computer records
it must be guarded against as carefully as fire. Flooding
has been one of the more common causes of damage to computer
centers, and has resulted from sources such as storms, broken
water or steam pipes, and water used in fighting fires. One
case in our sample where flooding caused extended water damage
was at the U. S. Postal Services ADP Center, Wilkes Barre,
Pennsylvania, in 1972.

On Saturday, June 24, 1972, water from the Susquehanna
River inundated all of downtown Wilkes-Barre and filled the
basement of the Post Office Building. Water continued rising
until about 6 inches of it were on the computer room floor.
About $7.5 million worth of Government computer equipment
is located on raised flooring on the first floor. Had the
water risen just an inch or so more it would have ruined
almost all of the computer equipment. (See pp. 12 and 13.)

11
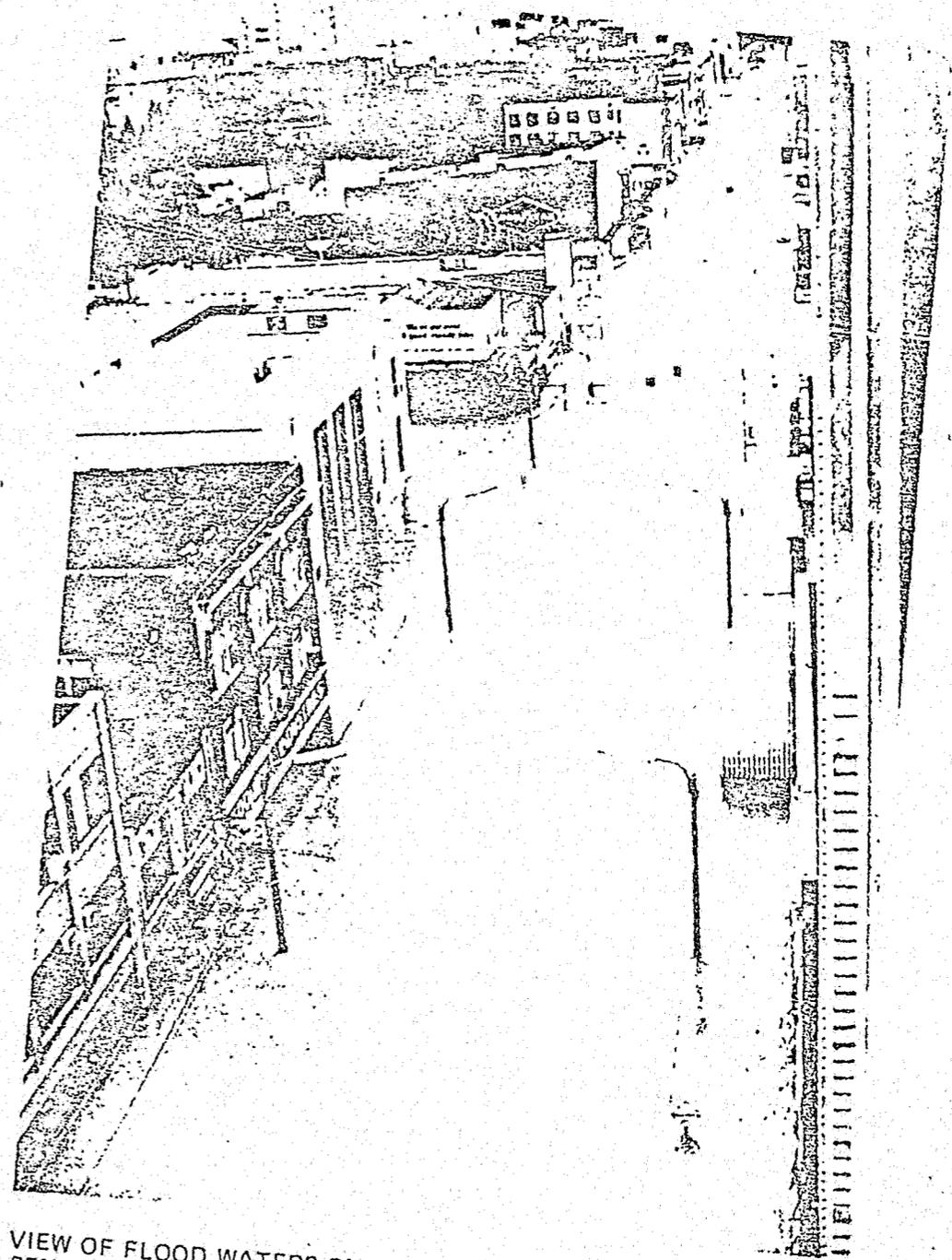
VIEW OF FLOOD WATERS ON SOUTH MAIN STREET, WILKES-BARRE, PENNSYLVANIA. POSTAL ADP CENTER IS LOCATED IN THE WHITE BUILDING ON THE LEFT.

(Courtesy of Bell Telephone Company)
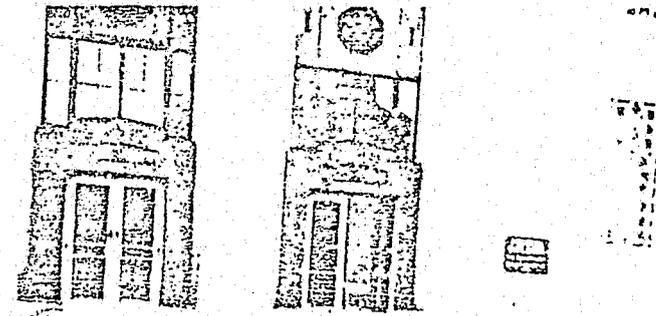
FRONT VIEW OF WILKES-BARRE POSTAL
ADP CENTER ON SOUTH MAIN STREET.
(Courtesy of U.S. Postal Service)
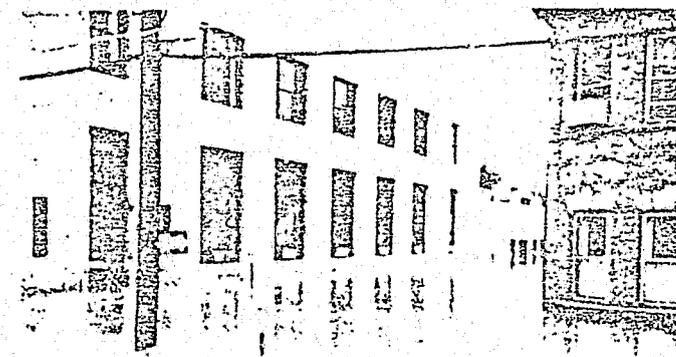


SIDE VIEW OF WILKES-BARRE POSTAL
ADP CENTER.
(Courtesy of U.S. Postal Service)

13

However, extensive damage was done to the building, communication lines and equipment, backup power supply, and all data processing supplies stored in the basement. Cleanup procedures required to place the data processing facility back in operation involved

   --replacing all communication equipment and computer supplies,

   --drying out and cleaning computer equipment,

   --making extended building repairs, and

   --removing over 90 dump-truck loads of silt and debris from the building. (See p. 15.)

Water also was responsible for much of the damage in the Pentagon bomb incident in May 1972. (See p. 20.) In this case the computer facility was flooded from broken overhead water pipes.

During our study we identified 10 locations where computers were operating where overhead water pipes existed without adequate provisions for drainage. Also, two locations were identified where computers were operating in basements which were below ground level. (See p. 6.)

SABOTAGE

Sabotage is another problem with which many Government agencies must be concerned. For instance, on August 24, 1970, a bomb exploded outside the Sterling Hall Building at the University of Wisconsin. (See pictures on pp. 16 to 18.) This building housed the Army Mathematics Research Center and other federally funded research activities. One employee was killed and three others were injured from this incident. This explosion damaged 25 buildings at the university, and resulted in a total loss of about $2.4 million for buildings and equipment. Computers at the Army Mathematics Research Center were damaged, and some programing efforts and 20 years' accumulated data was destroyed. It has been estimated that this research data represented over 1.3 million staff hours of effort which we calculate to represent an investment of about $16 million.

Because of this incident, the university strengthened its physical security measures by increasing the number of security guards and the activities of security patrols by adding a bomb squad and by placing greater restrictions on access to campus buildings.
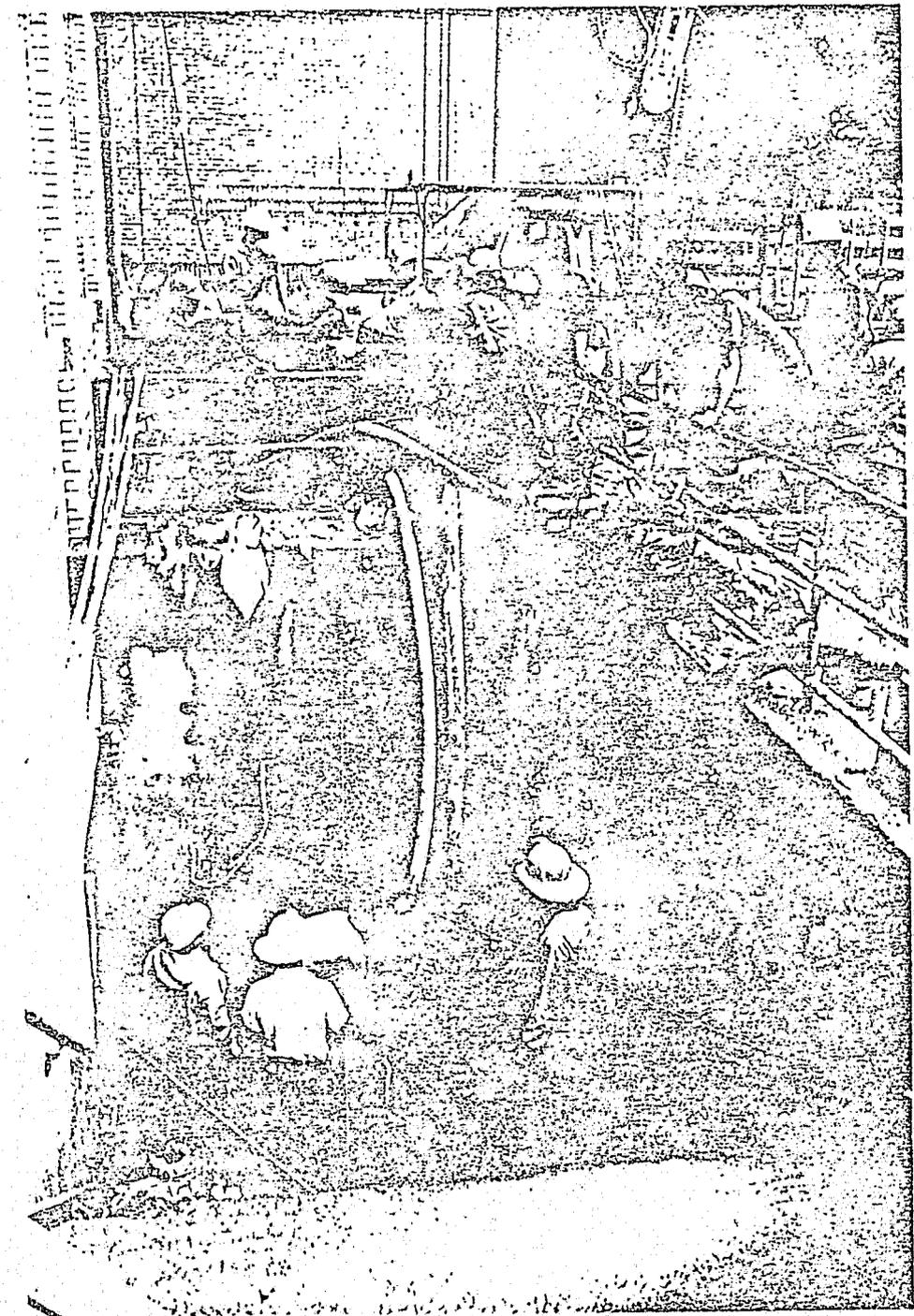
VIEW OF CLEAN-UP OPERATIONS ON SOUTH MAIN STREET,
WILKES-BARRE, PA., AFTER FLOOD

(Courtesy of Bell Telephone Company)
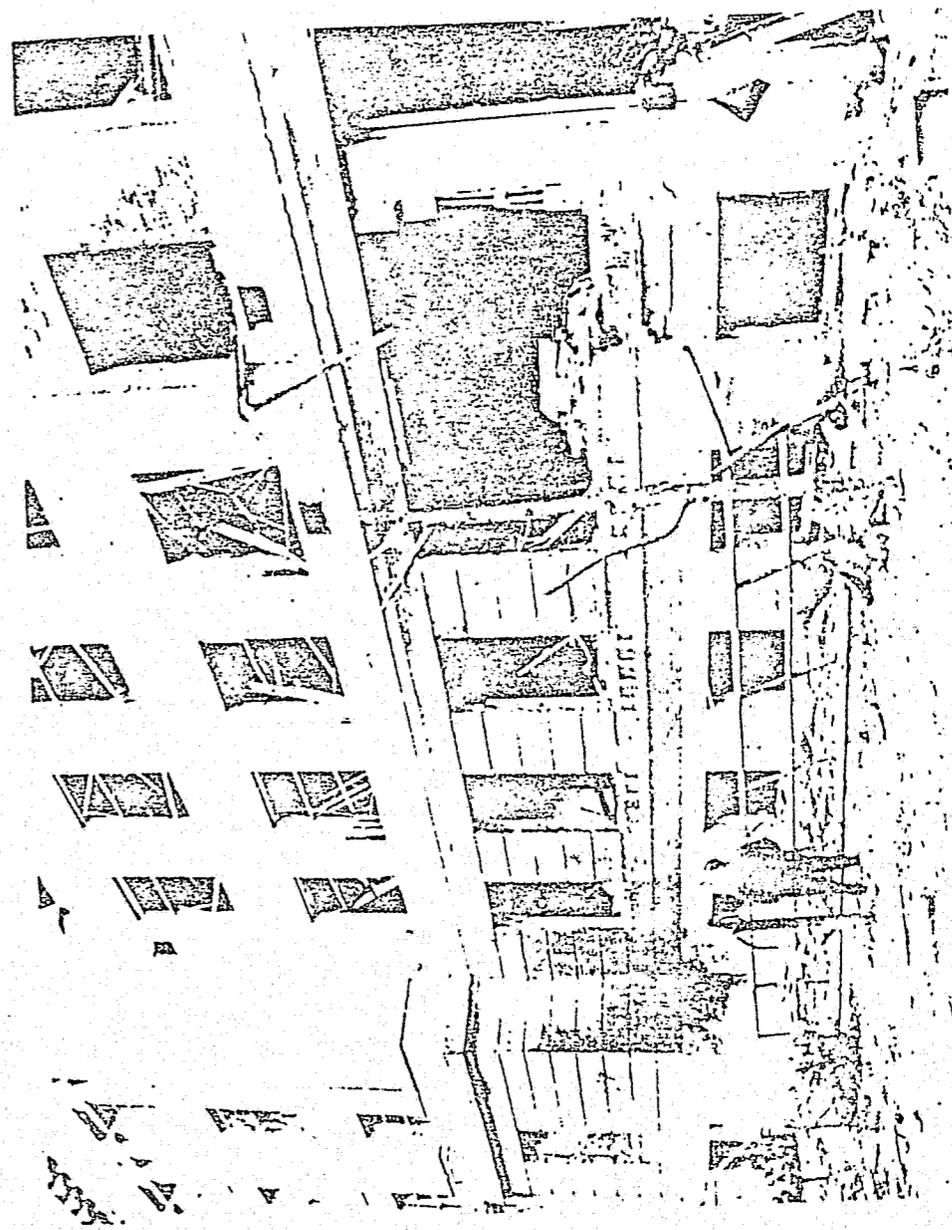
VIEW OF DAMAGE DONE TO COMPUTER BUILDING BY BOMB EXPLOSION
OUTSIDE THE ARMY MATHEMATICS RESEARCH CENTER
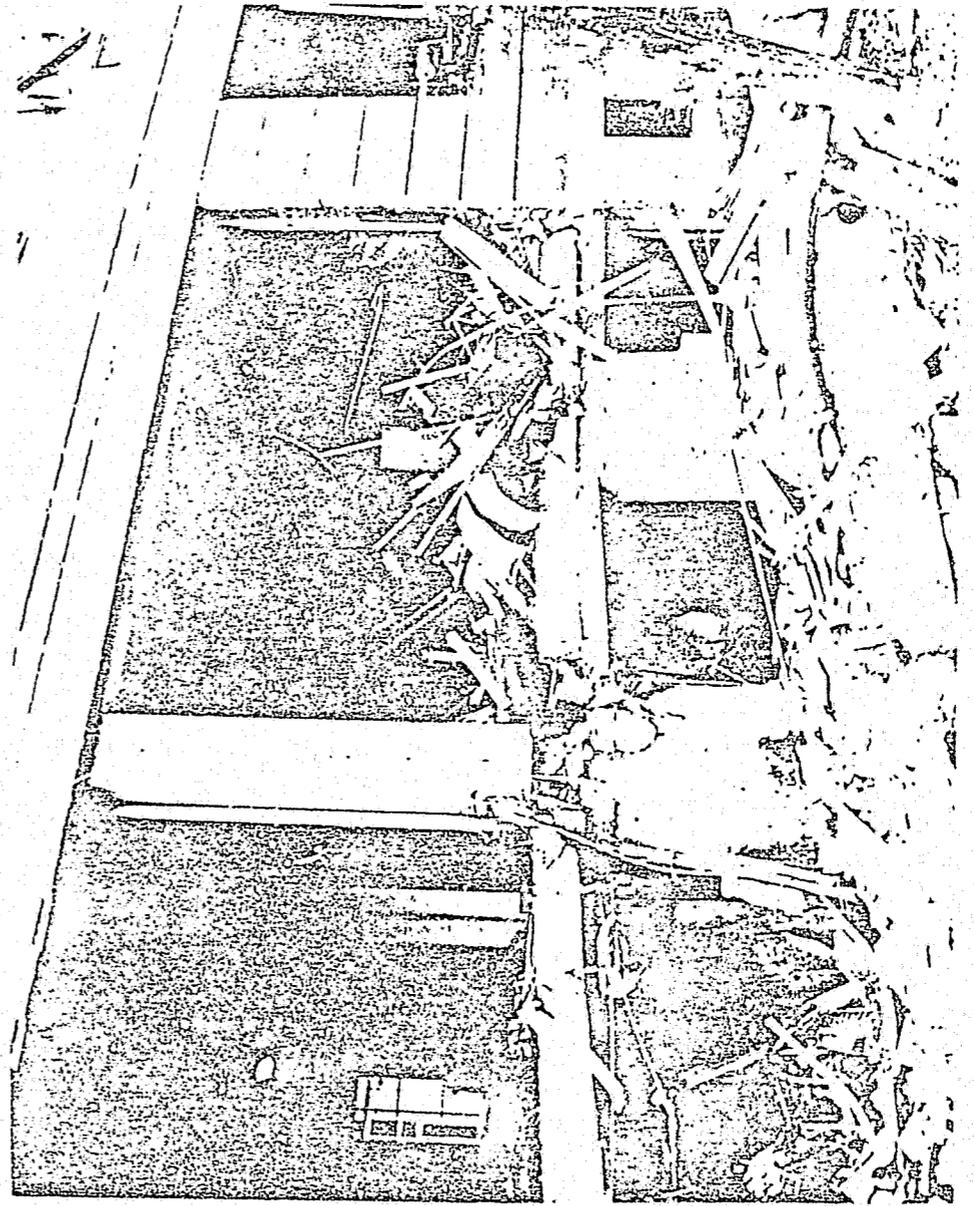
CLOSE-UP VIEW OF DAMAGE DONE TO EQUIPMENT AND BUILDING BY BOMB
EXPLOSION AT ARMY METHEMATICS RESEARCH CENTER

17
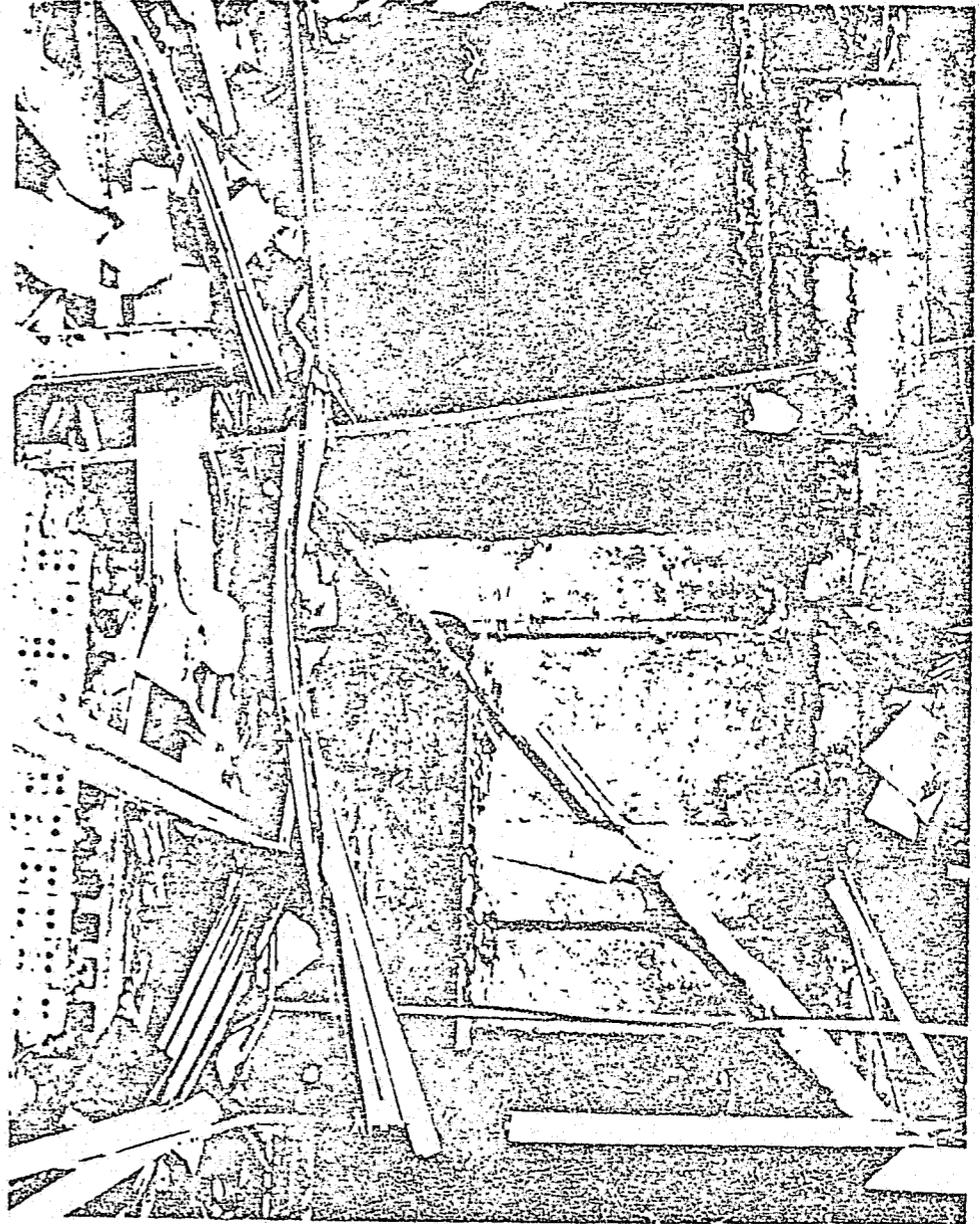
CLOSE-UP VIEW OF DAMAGE DONE TO EQUIPMENT AND BUILDING BY BOMB EXPLOSION AT ARMY MATHEMATICS RESEARCH CENTER

During May 1972 a bomb exploded on the fourth floor of the Pentagon above the computer facility and caused extensive damage. The computer facility was flooded from broken water pipes and parts of it were inoperable for about 29 hours. (See picture on p. 20.) In addition to cleanup costs, a $21,900 removable disk storage unit had to be replaced because of this incident. The director of data automation subsequently requested that a suitable means be developed for diverting any future overhead water flow away from the computer area.

During our study we identified locations which were susceptible to sabotage (see p. 6) by not supervising service personnel while on the premises or in the computer areas. Three computer locations were also possible targets for vandals.

Attempts at sabotage of ADP activities have also been made by employees within data processing centers. For example, there were four attempts to sabotage computer operations at Wright-Patterson Air Force Base during a 6-month period ending November 15, 1974, by using magnets, loosening wires on the computer mainframe, and gouging equipment with a sharp tool. Although the financial loss from these attempts was relatively small, the local management reacted by adding controls to limit access to the computer facility and also to limit personnel traffic to authorized areas within the computer installation.

THEFT OR MISUSE

Computerized systems are also vulnerable to theft or misuse by wrongdoers. We noted numerous cases of publicized thefts or misuses involving

--data or assets,

--financial frauds,

--embezzlements, and

--mistakes made by computer employees.

Industry literature indicates thefts or misuses of computer systems are increasing at an alarming rate.

One case we noted during our study involved theft of Government funds at Kelly Air Force Base, San Antonio, Texas. The Government paid approximately $100,000 to bogus fuel companies for aircraft fuel never delivered to the Air Force. The bogus fuel companies were established by a dishonest
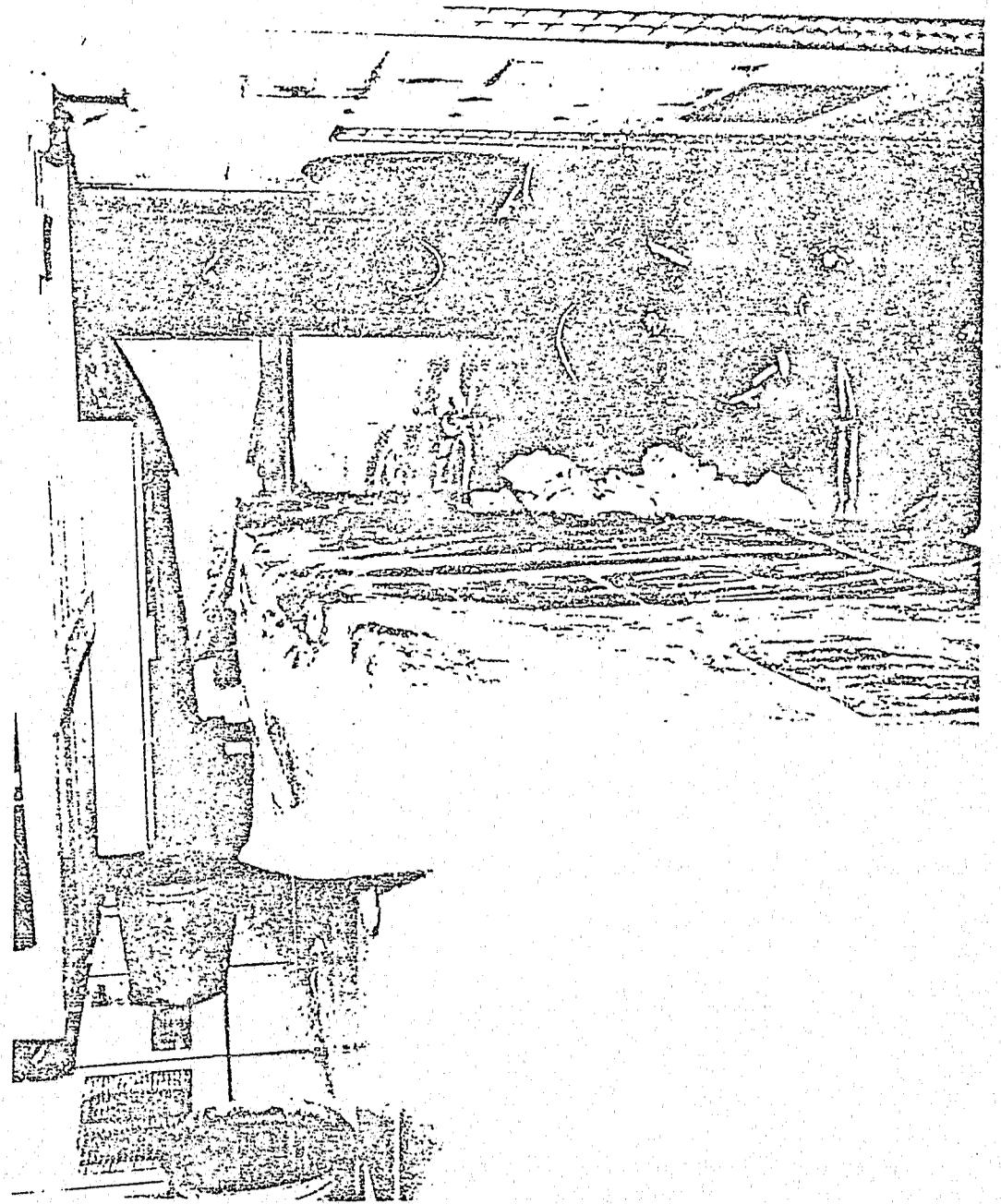
VIEW OF PENTAGON COMPUTER EQUIPMENT AFTER BOMB EXPLOSION
IN REST ROOM ABOVE THE COMPUTER FACILITY. PLASTIC WAS USED TO
PROTECT THE EQUIPMENT FROM DRIPPING WATER.

(Courtesy of Department of Air Force)

Government employee working at the air base. This employee
had indepth knowledge of the computerized fuel accounting
system which he helped develop and install. An investigation
of this matter was initiated when a bank contacted the Air
Force regarding suspicious banking transactions involving
Government checks. The employee was later arrested and
sentenced to 10 years in jail for theft of Government funds.

Other studies of theft and misuse to data processing
operations have been identified within the Federal Govern-
ment and private sectors. Noteworthy were March 1973 studies
by the Stanford Research Institute on "Threats to Computer
Systems" and a November 1973 study on "Computer Abuse."
Each study catalogued over 100 data processing security in-
cidents within and outside the Federal Government that were
identified from sundry sources. The study on "Threats to
Computer Systems" also recognized the problem of identifying
and solidifying security events at data processing installa-
tions and emphasized that a timelag phenomenon occurs in
identifying or reporting security events.

We did not attempt to determine which locations were
vulnerable to theft or misuse by Government employees at
the 28 locations we visited. However, we did identify five
locations where computer systems were in operation without
security procedures to detect improper or erroneous attempts
to use the computer or data files involved. (See p. 6.)

POWER FLUCTUATIONS

Unexpected surges or interruptions of electrical power
can cause serious damages to data and computer equipment.
In a computer operation which processes one job at a time,
computer instructions can store data during different job
stages, thus providing a limited degree of protection for
possible data distortions caused by power fluctuations.
The need for some form of power support or backup capability
becomes more apparent with on line or real time computer
systems because of the number of jobs or the mix of jobs
being processed at any point of time. These types of
computer systems become more vulnerable to losses caused
by power fluctuations.

The computer center at the National Institutes of Health,
Bethesda, Maryland, has experienced many computer system
failures which have been attributed directly to fluctuations
of electrical power. Officials of the computer center esti-
mate that they lost a minimum of $500,000 annually from elec-
trical power fluctuations. During a 5-week period, the com-
puter center experienced 6 major electrical power fluctuations
which caused 15 computer system failures. These failures

resulted in destruction of data for 375 batch processing jobs and for 2,250 remote terminal users. Moreover, these power fluctuations caused replacement of electronics costing over $94,000 in various components of the computer systems.

Our study showed that 4 out of the 23 data processing installations contacted have experienced problems caused by electrical power fluctuations and interruptions.

There are several alternative solutions to problems related to electrical power requirements. Some installations may be located in areas where they can change sources of power supply or use secondary sources of electrical power as backup; others may need to install electrical generating plants or uninterruptible power supply systems.

CONTINGENCY PLANNING

We found that only 13 of the 28 (less than 50 percent) of the Federal installations visited during our study had written contingency plans to insure continuity of data processing operations if a loss should occur. (See pp. 48 and 49.) Contingency planning is nothing more than developing a formalized plan of action to be taken in the event of work stoppage, physical damage, or when a loss occurs. Such plans are generally developed to cover minor disruptions as well as catastrophic events. A typical plan might include

--evacuating people,

--locking up files and facilities,

--turning off power, and

--making provisions for backup capabilities,

One case in our sample where losses did occur was at the Postal Service ADP Center, Wilkes-Barre, Pennsylvania. (See p. 7.) However, these losses were not catastrophic because the Postal Service had a contingency operating plan to minimize losses and continue operation.

This post office is an important cog in the postal data processing operation which services about 200,000 postal employees in 67 post offices in the Eastern and Southwestern areas of the United States. The office collected data on time and attendance for Postal Service employee payrolls, maintained labor distribution information, and gathered data on mail volume.

Although the flood occurred at the end of a pay period, the office was able to continue with its data processing function at a backup site. The workload and payroll targets' were met with a minimum number of problems and the facility was back in operation in a little over 2 weeks. Some contingency procedures used during the flood were

--removing master and other important tape files needed to continue operations to the backup facility when the water was inundating the ADP facility,

--making provisions for processing the most critical ADP operations at the backup facility, and

--taking necessary protection procedures to guard against flood damage when the water was rising.

The fire loss at the St. Louis Records Center is an example of what can happen when contingency plans are not made. About 16.8 million master military personnel records were lost in the 1973 St. Louis fire.

This installation's mission is to maintain these official Government records and to respond to inquiries made by the Congress, other Government agencies, and the taxpayer. This mission will now be hampered for some time because the lost records--some of which may be irreplaceable--must be reconstructed to satisfy inquiries, which is a costly and time-consuming process. (See pp. 24 and 25.)

While it is unreasonable to expect that there would be backup for every original record in the manual files, it is reasonable to assume that some sort of contingency planning should have been done to insure continuity of operations when a loss has occurred. Agency officials told us that a contingency plan was formulated after the fire happened.

It is important to note that contingency planning and backup capabilities received a relatively low degree of concern at the Government installation we visited while the potential loss impact on individuals and organizations requiring data from computerized records was growing. Many catastrophic problems can now be caused by security losses to computer facilities.

Such problems could possibly occur at Government installations without proper security and the development and implementation of sound contingency plans for data processing activities. We hope the 14 locations we visited
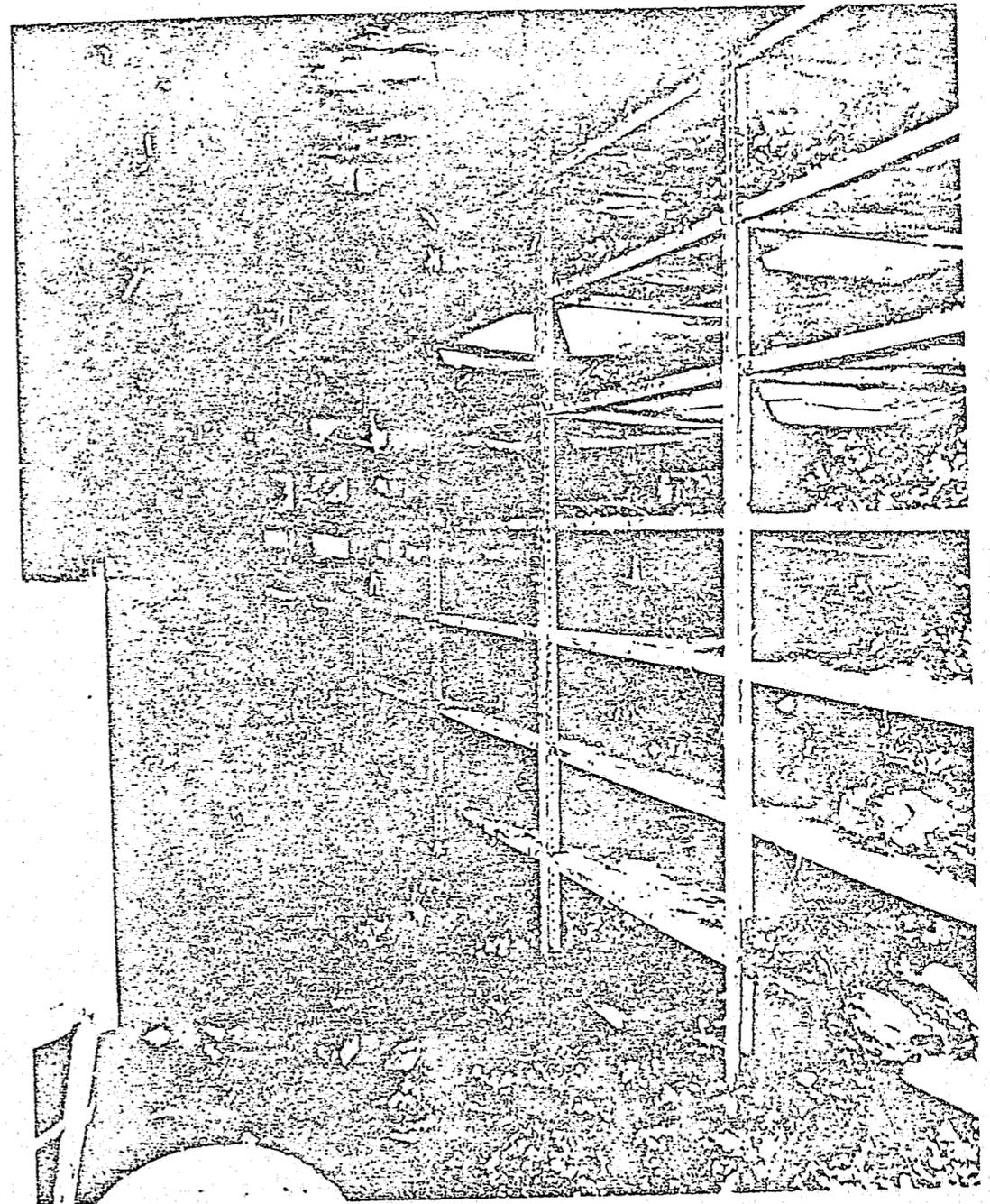
VIEW OF RECORDS DESTROYED IN ST. LOUIS FIRE.
RECONSTRUCTION WILL BE COSTLY AND TIME
CONSUMING DUE TO THE LACK OF CONTINGENCY PLANS.

(Courtesy of General Services Administration)
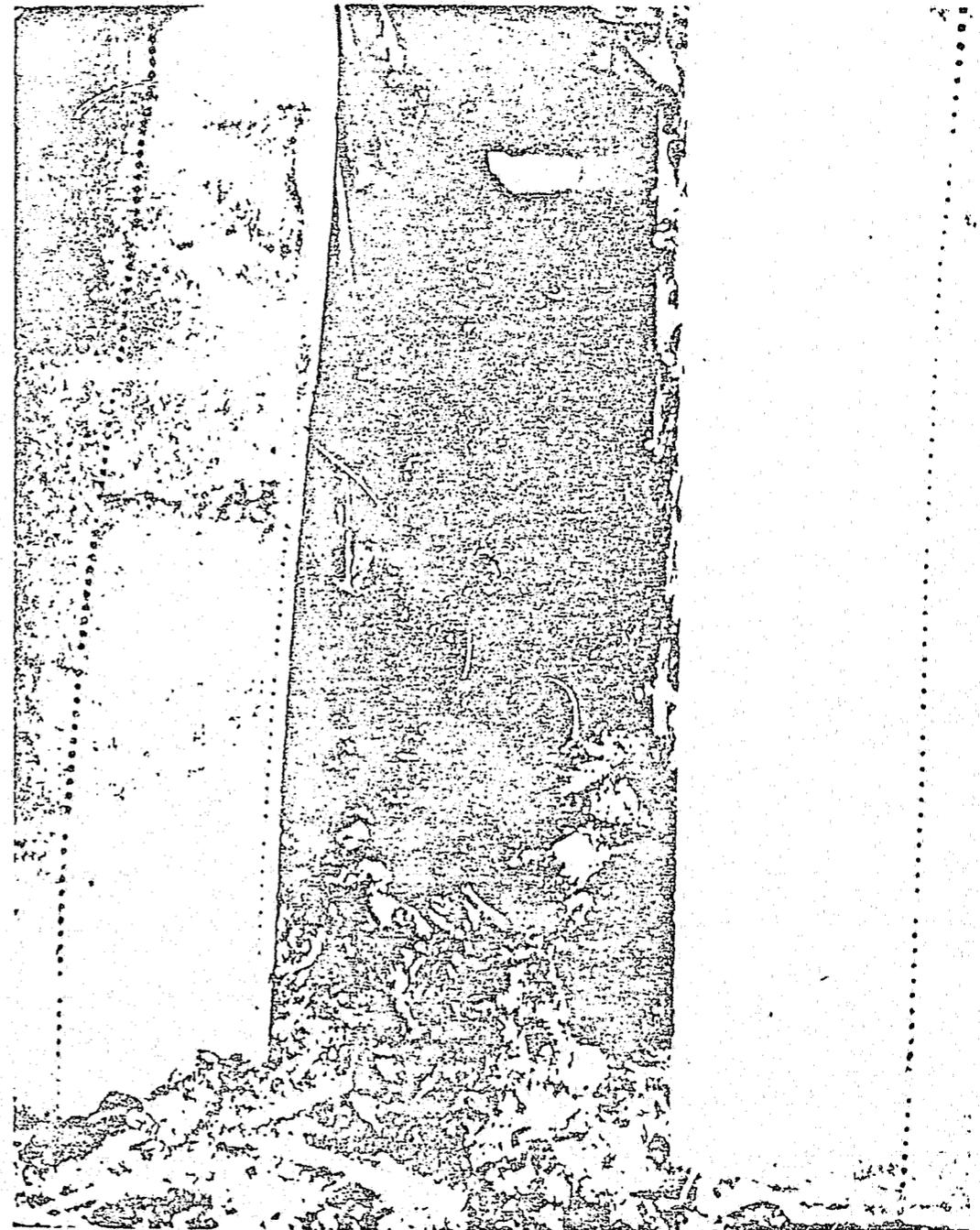
VIEW OF MORE RECORDS DESTROYED IN ST. LOUIS FIRE. SOME OF
THESE RECORDS MAY NEVER BY REPLACED

(Courtesy of General Services Administration)

25

which had no contingency plans to insure continuity of operations if a security event happened (see p. 6) will recognize their errors and develop contingency plans before a loss occurs and a plan is needed.

Other types of physical losses have occurred at Federal data processing installations. In some cases the losses were small; in other cases, they were costly and disruptive. The losses or damages were caused by earthquakes, windstorms, air conditioning failures, fires, and floods. Generally, the determining factors as to the extent of the loss--whether small or catastrophic--have a direct relationship to the intensity of the security event and to the amount of protection provided by the physical security program in use by the Federal agency.

# CHAPTER 3

## FEDERAL DATA PROCESSING SECURITY PRACTICES

In our visits to 28 Federal installations we found that there was great diversity in the security practices employed. These practices ranged from minimal physical protection given to computers operated in an unguarded warehouse not designed for computers to very complex security measures for certain data processing centers. For the most part, Federal agency security practices have been based on:

--Data processing managers' reactions to losses that have occurred.

--Information gathered from reading technical publications or attending conferences or meetings.

--Suggestions made by agency policies such as Department of Defense Security Manual 5200.28-M.

--Recommendations made by computer manufacturers.

We found that the responsibility for data processing security was usually left to local managers of computer centers even though the data processing assets and activities involved all facets of the organizations. Security measures were usually installed by managers of data processing installations with little or no study or evaluation to determine if such devices provided the proper level of protection needed. Some installation managers were not sure whether or not their installations were over- or under-secured.

## GOVERNMENT-WIDE GUIDANCE

During 1974, while we were visiting Federal installations, NBS issued Federal Information Processing Standard Publication 31, titled "Guidelines for Automatic Data Processing Physical Security and Risk Management." These guidelines should go a long way in aiding Federal officials in making and justifying essential security decisions. The guidelines were not available to those installations visited during the early days of our study. For this reason, the installations visited usually told us that there was no Government-wide guidance available for their use in the security area. (See app. IV for summary.)

It was too early to evaluate the effect of these new guidelines on Federal agencies security practices. However, we did study and review these guidelines and can say that

27

they cover in detail numerous subjects for use by Federal
organizations in structuring physical security programs for
their ADP 'facilities.  The publication discusses security
analysis, natural disasters, supporting utilities, system
reliability, procedural measures and controls, offsite
facilities, contingency plans, security awareness, and
security audit.

We don't believe these guidelines adequately covered

--where responsibility for physical security should be
assigned and

--when and where the guidelines should be used.

## RESPONSIBILITY FOR PHYSICAL SECURITY

The NBS publication is intended to provide guidance
for planning a security program and therefore is directed
to the security planner(s).  It suggests procedures for
developing and implementing a physical security program
by analyzing risks, reducing exposures to losses, planning
for contingencies, training personnel, and reviewing and
adjusting the program.

The NBS publication does not direct much attention to
the day-to-day job of seeing that the security program is
properly maintained and does not specify where that responsi-
bility should be in the organization.

Recognized experts believe that security is too
important to be considered merely one of several operating
functions assigned to data processing managers.  Generally,
data being processed originates and ends outside the data
processing facility; thus, there is an overall valid concern
for the proper level of security over this valuable facility.

In our opinion, the responsibility for physical
security needs to be assigned to a management level official
of the organization who is not operationally responsible for
the data processing facility.  Such an individual should

--be sufficiently knowledgeable of the operations and
programs of the agency to understand the value of
data and data processing facilities,

--be sufficiently high in the organization to see the
potential adverse effect losses of data processing
facilities could have on the mission of the agency,

28

--have the necessary authority and responsibility to
   establish policy and to manage all aspects of the
   security program, and

--be knowledgeable of new technology for ADP security.

## GUIDELINES SHOULD APPLY TO ALL FEDERAL INSTALLATIONS

The Bureau's guidelines are directed toward new automatic data processing systems being developed or improvements being made to existing systems. There is no requirement for applying the guidelines to all existing data processing operations.

Since December 31, 1975, the Federal Government has been using about 9,000 computers in its day-to-day operations. Because of the security events that have occurred, we believe that Federal managers need to develop a physical security and risk management program which will implement the most cost-effective security practices at existing as well as new data processing activities.

The guidelines concentrate primarily on physical security measures for protecting equipment, personnel, and data at the computer site. Very little mention is made of the data processing activities that can be performed outside the computer center. For example, activities such as data collection, data preparation, and distribution of output to end users are important functions in a data processing operation which, in many instances, are performed outside the computer center. The guidelines fail to adequately cover these important areas and need to be strengthened to insure that adequate protection is provided.

# CHAPTER 4

## CONCLUSIONS, AGENCY COMMENTS, AND OUR

## EVALUATION AND RECOMMENDATIONS

### CONCLUSIONS

Although perfect security is generally regarded as unattainable, we believe that there is a need for a high degree of insurance that data processing assets and valuable data are properly protected and that there are contingency plans to insure continuity of operations if a loss should occur. Adequate protection is needed because of the:

--Substantial investments in data processing assets and data.

--Value of data processing assets to the successful accomplishment of agency mission or goals.

--Potential for loss of irreplaceable Government records and its impact on those who rely on such records.

--Federal laws requiring that data processing . sets be protected from theft, alteration, destruction or misuse.

Our study showed that computer security practices in the Federal Government have not provided the necessary insurance that data processing assets are properly protected.

We attribute the poor security measures to a general lack of concern for a comprehensive plan to provide effective security at a reasonable cost. As discussed in chapter 3, NBS in 1974 published physical security and risk management guidelines for Federal agencies when planning security measures for new or improved data processing installations. However, no policy statement has been issued by OMB regarding the application and use of the guidelines.

The NBS guidelines include details on how to protect against such threats as loss from fire, flood, sabotage, and theft, and how to decide what measures to apply in what circumstances. They also advocate a concept of risk management; that is, making a formalized assessment of the resources to be protected versus the cost to protect them and whether the cost involved is worth it.

30

We believe that the NBS guidelines as modified by our suggestions will provide the necessary means to structure a sound program and could go a long way in improving the conditions we found.

However, use of the NBS guidelines is not mandatory and they apply only to new installations or those which are improving their computer systems. Moreover, the guidelines do not and could not be expected to assign responsibility for this function to an appropriate management official.

## AGENCY COMMENTS AND OUR EVALUATION

Comments were o .ained from six Federal agencies (see app. III) on our proposals to strengthen physical security over computer systems. We proposed that the Director of OMB issue policy directing that

--specific assignments of responsibility for physical security of ADP systems be made at each Federal installation using computer systems and

--responsible officials use the NBS guidelines when developing physical security and risk management programs.

The Department of Health, Education, and Welfare, the Department of Transportation, and the U. S. Postal Service agreed with all our proposals. In fact, the Department of Health, Education, and Welfare and the Postal Service already have issued agency ADP security policies as we recommended in this report.

Other comments received generally concurred with our observations that improvement is needed in the physical security area; however, they differed on ways to correct or improve on the conditions found. Following is a summary of the comments.

## Proposal that a management
## official be appointed

The Assistant Secretary of Defense and three other agencies agreed with our first proposal and suggested appointing a management official who is highly knowledgeable in ADP and security matters as well as being independent from the direct management of the ADP facility for his purpose.

The Assistant Secretary for Science and Technology, Department of Commerce, however, did not agree with our

31

proposal and suggested that the ADP security responsibility be assigned to two different functional areas--the data processing department and the internal audit group. She suggested that the ADP organization should determine the security requirements while the audit functions should review the adequacy of the security safeguards and procedures.

The Director of OMB also questioned the proposal that a separate management official should be appointed and held responsible for ADP physical security. He said that the agency head is already responsible for protecting agency installations and that he should establish whatever safeguards are appropriate.

### Our views

We recognize that an agency head is responsible for its overall management and operation and this makes his day-to-day responsibilities most demanding. For this reason, we believe that he cannot spend much time on determining what measures are necessary as well as how to organize an effective security program. Since ADP is an important issue to the well-being of most agencies, we believe that the agency head should delegate this responsibility to a management official, if one has not been designated, who is knowledgeable in agency missions or goals as well as in data processing and security matters.

Also, we know that different circumstances exist at Federal agencies and that there are different organizational structures to satisfy security responsibilities. For example, at some agencies one person or a small staff is responsible while at other agencies a whole network of people may be required to handle the security requirements at the various installations which the agency maintains. For these reasons, it is difficult to prescribe the ideal organizational structure that would be needed at each agency to handle ADP security responsibilities. However, we do know that as a minimum a responsible management official should be assigned this responsibility at each computer installation and that he determine the proper levels of security needed under the existing circumstances.

As to the Department of Commerce comments we agree that the internal audit functions should review agency ADP security practices and procedures. However, we do not believe that the ADP organization should have the sole responsibility for determining what security practice and procedures are needed. ADP security is too important to be considered as one of several operating functions assigned to the ADP organization. At most agencies, computers are considered to be the single most important

32

tool for management; and the data they process involves almost all facets of the organization. For these reasons, we believe that establishing and managing ADP security requires time and attention of an independent management official who has the knowledge, responsibility and authority to insure that ADP activities are properly safeguarded at reasonable costs.

## Proposal that OMB issue policy instructions regarding use of guidelines

The Director of OMB questions whether it is necessary at this time for OMB to issue any further policy directives regarding the use of the NBS guidelines. He believes that it would be more appropriate for us to direct our recommendations to improvements needed in these guidelines and to the conditions found at the installations visited.

Public Law 89-306 assigns the Government-wide policy and oversight responsibilities for ADP management to OMB while Commerce is responsible for ADP technical standards. Current Government-wide ADP policies do not adequately cover ways or concepts to protect this annual multibillion dollar activity which permeates most facets of Government operations. According to the Director of OMB, this law and Executive Order 11717, dated May 9, 1973, gives NBS the responsibility and authority to develop, coordinate, and issue appropriate uniform ADP technical standards. Had NBS issued ADP security technical standards, we would have addressed our recommendation, relative to policy directives and their use, to NBS. The NBS guidelines, however, were issued as a reference document--not as an ADP technical standard.

The Assistant Secretary for Science and Technology. Department of Commerce, agreed to consider our suggested changes in the next edition of the guidelines. In this regard, the Assistant Secretary of Defense also voiced concern about the mandatory aspect of our recommendation. It is his view that the guidelines need further refinement before becoming a mandatory standard.

### Our views

We agree that the guidelines are still in the developing stages and must be refined further. However, unless the agencies use the guidelines it will be difficult to gain the experience needed to improve them.

Moreover, the NBS guidelines are not a rigid, unflexible set of rules. They instead provide matters to be considered in arriving at an intelligent, cost-effective approach to matching, risk against severity of possible loss. They are meant to be applied selectively. We believe they are a good vehicle to initiate Federal agencies in the use of sound physical security practices and risk management advocated in our report. Finally, we believe that the importance of good security for ADP's facilities outweighs any further delay for achieving a more perfect guidelines.

In summary, our review showed that responsibility was not clearly fix.d at installations we visited as to who should be held responsible for ADP security and what safe-guards were needed to adequately protect their ADP facilities against security threats. Comments received on this report from some of the agencies showed that this confusion still exists. Without a strong Government-wide policy requiring a systematical management approach for protecting ADP as-sets at reasonable costs, managers of data processing in-stallations, we believe, could continue the practices ob-served in this report which can result in installations being over- or under-secured.

## RECOMMENDATIONS

We recommend that, in order to provide more physical security over Government ADP operations at a reasonable cost, the Director of OMB issue policy directing that:

--Management officials be appointed at Federal installa-tions having data processing systems and that they be assigned responsibility for ADP physical security and risk management. Such officials should be aware of the impact of ADP operations on the organizations' mission or goals and the importance of the data and records to U.S. citizens 'nd the Federal Government. Also, the official should be knowledgeable in data processing and security matters.

--These officials use the NBS guidelines when developing and implementing physical security and risk manage-ment programs.

Also, since we believe that ADP security is an important matter, we are sending copies of this report to each Federal agency head for their information and use.

## A CONCEPT FOR USE

### IN

## MAKING SECURITY DECISIONS

The concept of risk management is one which we believe may be useful in deciding what security practices are cost effective. This concept has been used by industry and Federal agencies--particularly the insurance industry--to make decisions regarding the costs of protecting against possible losses. The approach also has been advocated by NBS in its publication entitled "Guidelines for Automatic Data Processing Physical Security and Risk Management."

We are presenting a description of the approach here so it can be considered by agencies who undertake improvement in the physical security of their computer systems.

### RISK MANAGEMENT

Risk management is an element of managerial science that is concerned with identification, measurement and control of uncertain events. This concept is not new, and portions have been used by organizations in quantifying needs when establishing business strategies. For example, one company used systematic risk analysis techniques to determine the extent of insurance coverage necessary for protection against product liability. This provided the company with a savings opportunity by assuming a $5 million aggregate loss deductible on a $6 million product liability insurance policy. In national defense, quantitative methods are used for analyzing risks to assure that proper safeguards are acquired and strategically implemented.

Portions of the risk management concept have also contributed to the insurance industry by providing greater flexibility in the type of insurance services offered for sale and wider ranges of insurance coverage at less cost to the industry. Risk management can also be used to determine an optimum level of security for data processing operations.

We contacted organizations referred to us as users of risk management techniques to determine security requirements. Some of these organizations considered factors used in risk evaluations but in most instances did not use a comprehensive risk management approach. Many leading

authorities in automatic data processing security are using
various methods for analyzing risks, and they consider the
following four phases essential for a formalized risk
management approach:

 --Risk analysis, management decision, risk control, and
   process continuity.

## Risk analysis

 Risk is the uncertainty of occurrence and outcome of
specific events.  Financially there are two basic types of
risks.

 --Speculative risks; an organization's investment of
   some or all of its assets with a degree of
   uncertainty as to whether the outcome will result
   in a gain, loss, or no change.

 --Pure risks;  unilateral events which could result
   in a loss of some or all of an organization's
   assets.  Such losses are generally caused by
   physical destruction, misplacement, theft, fraud
   or adverse legal action.  Uncertainty relates to
   whether or not a loss will occur; there is no
   opportunity in these instances for a financial
   gain.  Threats against security in Federal data
   processing operations are considered as pure risks.

 The initial planning for analyzing risks is to determine
the extent necessary to carry out the analysis.  Considera-
tion should be given to the

 --estimated costs and availability of funds to perform
   an analysis,

 --value of the physical installation,

 --worth of data to the organization and to others,

 --existing safeguards, and

 --impact of data processing on the organization's
   mission or goals.

Such considerations could dispose of the need for further
detailed analyses.  To illustrate, small computers used
as calculators generally would not require extensive analyses
because of their low cost and limited use for data storage.

Larger centralized time-sharing computer systems, however, would generally require risk analyses.

When a detailed analysis is warranted, all data processing assets such as computer equipment, software, and data, that are used to support a program or organizational goals must be identified and assigned a monetary value considering both the worth of the asset within and outside the organization.

An important phase in risk analysis is to identify all possible threats against assets. A risk audit is one technique used for this identification. A number of existing security checklists can serve as workable audit plans. Such audit plans should include interviews with key personnel, onsite inspections, as well as reviews of pertinent documents, records, and financial data to gain knowledge of operations and procedures and to identify the maximum number of threats involved.

Once known security threats have been defined, it is then necessary to postulate unknown threats and to measure the probability of occurrence for each threat. Some important parameters affecting such measurements and evaluations are

--cost and historical data on occurrence of various security threats,

--effectiveness of existing controls and procedures at an installation against each specific threat, and

--operating requirements both for the data processing activities as well as the organization.

Each type of security threat is unique and must be considered separately, as it can have a different impact on organizations. The levels of damage that can occur from each impact are referred to as loss severities. It is necessary to determine significant ranges of these severities for each threat. Once threats have been identified, it is then possible to determine the degree of loss and the impact of each loss on the installation's operating requirements as well as on the value of the facilities and data involved.

## Management decision

The data gathered during the risk analysis phase can be summarized and presented to top management for consideration. This summary should relate threat assessments to

asset analyses and existing controls and show a relationship
of each threat to the organizational mission and goals.

From this summary, management officials could then
determine those risks that could be tolerated by the organi-
zation and those which require some control.  Instances
may occur when risk analyses indicate a reduction in security
levels that are being maintained against certain threats,
thus providing for reduced security costs.  Other in-
stances may show where the potential impact from risks com-
bined with existing security techniques, if any, are accept-
able to management.  The only action necessary beyond this
point would be to insure the effectiveness of techniques
being employed.

## Risk control

Once management determines that threats are unacceptable,
the next phase is to control or avoid such risks by implement-
ing an optimum degree of security relative to cost and operat-
ing requirements.

Risk handling techniques can be categorized as .llows:

--Risk avoidance; a determination that the effects from
  threats and the probability occurrence is such that
  computerization is not warranted.  Care must be taken
  with this decision to insure an ability to satisfy
  organizational needs with efficient and effective
  alternative solutions.

--Risk transfer; an organization's desires to shift some
  or all of its financial responsibility for risks to
  another party through contractual agreements.

--Risk assumption; a determination that it is more
  economical or operationally impractical to avoid the
  risk or transfer some portion of it to another party.

Federal Government policy is to absorb all financial
losses incurred.  Thus, specific methods must be identified
to minimize the severity of a loss from each risk.  Each
method should be evaluated in terms of its effectiveness and
cost and presented for management consideration.

## Process continuity

Once security techniques have been implemented, they
must be reevaluated periodically to determine their effective-
ness in relation to the organization's mission and to the

program's computerized activity. During this analysis, management should be alert to the possibility that both existing or proposed security systems could be in excess of actual needs. This aspect could be assisted by the internal auditor. He would report his observations to the risk manager. When such instances are noted, consideration should be given to the potential for cost savings by reducing the degree of security being employed.

## NEED FOR A RISK MANAGER

When computerized data serves the needs of more than one division or group, each program manager has a vested interest in the security of his data. If such a manager is permitted to establish separately his own security requirements, the resulting degree of security for data processing operations could become unmanageable.

The initial step in establishing a risk management system is to create a position for a risk manager. The system is not likely to succeed without having one knowledgeable individual responsible for decisionmaking and supervision over all technical and analytical activities in the process. In small organizations, this position could be assumed as a collateral one by a top level management official. In larger and more complex entities, however, a separate position sufficiently high in an organization should be established for a risk manager to have authority for data processing security across organizational lines.

Some of the requisites for a top-level risk management position should be

--knowledge of short- and long-range goals of the organization;

--awareness of users' security needs and priorities to establish and maintain appropriate levels of security;

--awareness of new technology for security;

--authority to make, or assist in making, policy decisions on security programs and procedures;

--authority, with management approval, to implement security measures deemed feasible from a risk analysis; and

39

--ability to follow through periodically on security
policies and practices in action, checking actual
performance and results.

Recognized authorities in risk management and automatic
data processing security matters both in Government and
industry agree that use of the risk management concept will
provide methodologies and the systematic approach necessary
for developing and maintaining proper levels of security
for data processing operations.

# CONTINUED

# 1 OF 2

# CONCEPT OF RISK MANAGEMENT

**ASSET ANALYSIS**
VALUE TO ORGANIZATION
VALUE TO OTHERS

**MISSION OR GOAL**
FOR ORGANIZATION
FOR ACTIVITY OR PROGRAM

**THREAT IDENTIFICATION**

**THREAT ASSESSMENT**
PROBABILITY OF OCCURANCE
SEVERITY
EXISTING SECURITY CONTROLS

**SUMMARIZE FINDINGS FOR MANAGEMENT**
RELATE FINDINGS OF THREAT ASSESSMENT TO ASSET
ANALYSIS AND TO MISSION GOAL

**MANAGEMENT DECISION**
ACCEPTABILITY OF IMPACT FROM THREAT
(BASED ON RISK ANALYSIS)

**ACCEPTABLE**
MAKE NO CHANGE
CONTINUE AS IS

**NOT ACCEPTABLE**

**PRIORITIES**
IDENTIFY THREATS BY
ORDER OF IMPORTANCE

**EVALUATE METHOD FOR
HANDLING THREAT**
AVOID BY NOT USING COMPUTER
TRANSFER TO THIRD PARTY
ASSUME LIABILITY

**PERIODIC RE-EVALUATION**
POTENTIAL IMPACT FROM THREATS
EXISTING SECURITY
NEW TECHNOLOGY

**IDENTIFY SECURITY TECHNIQUES**
TO REDUCE OCCURRANCE AND/OR
SEVERITY OF THREAT

**EVALUATE
COST/EFFECTIVENESS**
FOR EACH SECURITY TECHNIQUE

**RISK ANALYSIS**
**MANAGEMENT DECISION**
**RISK CONTROL**
**PROCESS CONTINUITY**

**SELECTION AND
IMPLEMENTATION**
MANAGEMENT APPROPAL
TEST AFTER IMPLEMENTATION

41

## SUMMARY OF SECURITY AREAS COVERED

## AT 18 FEDERAL DATA PROCESSING INSTALLATIONS VISITED

|  | Installations | | |
|---|---|---|---|
|  | Yes | No | N/A (note a) |
| **Access control:** | | | |
| Is the location | | | |
| --target for vandals? | 3 | 15 | - |
| --advertised? | 6 | 12 | - |
| --screened from the street? | 15 | 3 | - |
| Are guards at entrances? | 15 | 3 | - |
| Are photo-badge systems used? | 13 | 5 | - |
| Are visitors controlled? | 15 | 3 | - |
| Do employees challenge unfamiliar visitors? | 16 | 2 | - |
| Are entrance security devices used? | 11 | 7 | - |
| Is access to computer limited during | | | - |
| --working hours? | 17 | 1 | - |
| --off-shift hours? | 15 | 3 | - |
| **Fire exposure:** | | | |
| Are fire resistant/noncombustible materials used for | | | |
| --buildings? | 17 | 1 | - |
| --partitions, walls, doors? | 16 | 2 | - |
| --furnishings? | 15 | 3 | - |
| Are smoke detectors installed? | 11 | 7 | - |
| Do the smoke detectors turn off air-conditioning facilities automatically? | 6 | 5 | 7 |
| Is the smoke detector system tested periodically? | 7 | 4 | 7 |

a/Does not apply to installation and/or installation management that was reluctant to discuss these aspects of data processing security.

|  | Installations | | |
|---|---|---|---|
|  | | | N/A |
|  | Yes | No | (note a) |
| Fire exposure: | | | |
| Do fire extinguishers use | | | |
| --automatic carbon dioxide? | 2 | 16 | - |
| --halogenated agent? | | 18 | - |
| --water? | 7 | 11 | - |
| Are personnel trained for firefighting? | 10 | 8 | - |
| Is smoking restricted in computer area? | 13 | 5 | - |
| Are fire drills conducted regularly? | 11 | 7 | - |
| Are emergency power switches located at exits? | 16 | 2 | - |
| Do emergency power switches include air-conditioning system? | 11 | 7 | - |
| Flood control: | | | |
| Are computers located below water grade? | 2 | 16 | - |
| Do overhead steam or water pipes exist? | 14 | 4 | - |
| Does adequate drainage exist | | | |
| --under raised floors? | 4 | 12 | 2 |
| --on floors above? | 1 | 14 | 3 |
| --for adjacent areas? | 4 | 12 | 2 |
| Housekeeping: | | | |
| Are flammable materials properly stored? | 18 | - | - |
| Is area under raised flooring cleaned regularly? | 4 | 12 | 2 |
| Are paper and supplies stored outside computer room? | 15 | 3 | - |
| Are tapes and disks stored outside computer room? | 8 | 9 | 1 |
| Electric power: | | | |
| Is electrical power supply considered reliable? | 18 | - | - |
| Are voltmeters used to monitor supply? | 8 | 10 | - |

| | Installations | | |
|---|---|---|---|
| | Yes | No | N/A (note a) |

Air conditioning:

Is air-conditioning dedicated
  to computer area? 16 2 –
Are backup air-conditioning
  facilities available? 5 13 –

Personnel considerations:

Are employee background checks
  performed? 16 2 –
Are background checks updated
  periodically? 11 4 3
Is continuing education pro-
  vided for security matters? 10 8 –
Is one person responsible for
  managing security? 13 5 –
Has security policy been de-
  veloped? 15 3 –
Is in-house service personnel
  traffic
--controlled in vital areas? 13 5 –
--supervised? 10 8 –
Is a list prepared for
  authorized vendor service
  personnel? 14 3 1
Is positive identification re-
  quired for vendor service
  personnel? 15 2 1
Are vendor service personnel
  supervised while on premises? 10 7 1
Are vendor employee background
  checks verified? 5 8 5

Hardware considerations:

Are hardware operations compared
  to scheduled activities? 14 1 3
Are meter hours correlated with
  reported utilization hours? 10 7 1
Are all periods of reported down-
  time verified? 17 – 1
Is all incoming work checked
  against an authorized users
  list? 13 3 2
Is output spot checked for pos-
  sible misuse? 15 2 1

44

|  | Installations | | |
|---|---|---|---|
|  | Yes | No | N/A (note a) |
| Hardware considerations: | | | |
| Are output distribution lists updated periodically? | 9 | – | 9 |
| Are tapes cleaned at regular intervals? | 1? | 6 | 2 |
| Are tape utilization records maintained? | 10 | 7 | 1 |
| Is magnetic detection equipment used? | – | 17 | 1 |
| Software considerations: | | | |
| Is vital software and documentation secured? | 14 | 3 | 1 |
| Are backup files maintained at a secondary site? | 12 | 5 | 1 |
| Is access to essential software restricted on a need-to-know basis? | 16 | 1 | 1 |
| Is multilevel access control to files provided by | | | |
| --levels of security? | 3 | 9 | 6 |
| --breakdowns within files? | 4 | 8 | 6 |
| --restrictions for read-only, write-only, and update? | 6 | 6 | 6 |
| Are security software utilities and access codes validated periodically? | 4 | 6 | 8 |
| Is a monitor log maintained for those who access data banks or sensitive files? | 2 | 8 | 8 |
| Is a software security routine used to monitor unauthorized attempts to access files? | 2 | 7 | 9 |
| Are passwords utilized to identify users of terminals? | 6 | – | 12 |
| Are passwords changed frequently? | 4 | 2 | 12 |
| Are terminal users restricted to high-level languages? | 2 | 4 | 12 |
| Do operating systems have built-in protection to prevent the bypassing of other software security techniques? | 2 | 8 | 8 |

45

|                                                                | | No | N/A (note a) |
|----------------------------------------------------------------|--|----|--------------|

**Software considerations:**

| | | | |
|---|---|---|---|
| Are memory bounds in operating system software tested following maintenance and program loading? | 5 | 6 | 7 |
| Are restart and recovery procedures used in applications programs? | 15 | 2 | 1 |
| Do restart procedures ... on random as well as ...ntial files? | 7 | 4 | 7 |
| Are programing changes documented and controlled? | 16 | 1 | 1 |

**File considerations:**

| | | | |
|---|---|---|---|
| Are duplicate program files stored offsite? | 9 | 9 | - |
| Are fire-resistant containers used for storage of program files? | 13 | 5 | - |
| Is a current inventory of program files maintained? | 17 | 1 | - |
| Have program files been tested on backup facilities within past 3 months? | 7 | 10 | 1 |
| Are computer programing changes controlled? | 17 | 1 | - |
| Are programing changes made on a duplicate rather than the original program file? | 11 | 6 | 1 |
| Are items taken from files recorded? | 14 | 3 | 1 |
| Are duplicate copies of documentation maintained? | 13 | 5 | - |
| Are copies of documentation stored offsite? | 6 | 5 | 7 |
| Is fire-resistant storage equipment used for documentation? | 11 | 6 | 1 |
| Are backup copies of documentattion reviewed periodically to assure applicability? | 12 | 4 | 2 |
| Are all data files physically controlled by the computer center rather than the user? | 10 | 8 | - |

|                                                      | Installations | | |
| --- | --- | --- | --- |
|                                                      | Yes | No | N/A (note a) |
| **File considerations:** | | | |
| Are data files classified by degree of sensitivity? | 2 | 11 | 5 |
| Are data files stored outside the computer room? | 10 | 7 | 1 |
| Is the storage area for data files fire protected? | 9 | 6 | 3 |
| Is access to storage area for data files specifically controlled? | 7 | 9 | 2 |
| Are fire-resistant containers used for storage of data files? | 8 | 8 | 2 |
| **Resource sharing considerations:** | | | |
| Are remote terminals used only by selected individuals? | 4 | 1 | 13 |
| Is access to remote terminals controlled by | | | |
| --locked doors? | 1 | 4 | 13 |
| --posted guards? | 1 | 4 | 13 |
| --other restraints? | 3 | 2 | 13 |
| Are passwords used to identify specific terminals and users? | 6 | – | 12 |
| Is password system considered tamperproof? | 2 | 4 | 12 |
| Are passwords changed frequently? | 4 | 2 | 12 |
| Is access to password file restricted? | 6 | – | 12 |
| Does system software restrict time sharing users to specific data files? | 6 | – | 12 |
| Is right to add, delete, or modify files limited by software controls? | 6 | – | 12 |
| Does time-sharing software record all activity against a data file? | 3 | 3 | 12 |
| Is there software protection for online operating systems and applications programs? | 5 | – | 13 |

|  | Installations | | |
|  | Yes | No | N/A (note a) |
|---|---|---|---|
| Resource sharing considerations: | | | |
| Are security override proce- dures classified at the highest level and use of overrides monitored closely? | 5 | 1 | 12 |
| Is time-sharing security system monitored and reviewed? | 3 | 2 | 13 |
| Is debugging of security system closely monitored and con- trolled? | 3 | 1 | 14 |
| Contingency planning and backup: | | | |
| Does the installation have a formal written contingency plan? | 9 | 8 | 1 |
| Does the installation have a contingency training program? | 5 | 8 | 5 |
| Is a backup computer available? | 7 | 11 | – |
| Is the backup computer in the same room as the operating computer? | 4 | 4 | 10 |
| Can the backup facility handle the current workload? | 4 | 6 | 8 |
| If no designated backup, does center have access to another computer | 3 | 5 | 10 |
| Is an implementation plan avail- able for use of backup installation? | 8 | 6 | 4 |

## SUMMARY OF SELECTED SECURITY AREAS COVERED

## AT OVERSEAS DATA PROCESSING INSTALLATIONS
## VISITED

|  | Installation | |
|---|---|---|
|  | Yes | No |
| Are buildings originally designed for computers? | 1 | 9 |
| Are supplies stored in a separate room? | 7 | 3 |
| Are fire extinguishers located in the computer room? | 9 | 1 |
| Are smoke or heat detectors installed in computer room? | 6 | 4 |
| Are fire alarm pull boxes located in computer room? | 6 | 4 |
| Are there master power shutdown controls for computer room? | b/7 | 3 |
| Is emergency lighting installed in computer room? | 8 | 2 |
| Do buildings have water leakage problems? | 5 | 5 |
| Are separate air-conditioning facilities used for computers? | 8 | 2 |
| Are backup generators installed to insure reliability of electric power supply? | c/7 | 3 |
| Have formal contingency plans been developed for computer backup capability? | 4 | 6 |

b/One switch located in locked box, so not readily usable.

c/Backup generator at one location did not work at time of visit.

49

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

MAR 12 1976

Mr. D. L. Scantlebury
Director, Division of Financial
  and General Management Studies
General Accounting Office
Washington, D.C.  20548

Dear Mr. Scantlebury:

We have reviewed GAO's draft report, "Federal Managers Need
to Provide Better Protection for Automatic Data Processing
Facilities," as requested in your letter of February 10,
1976; and believe that the report is useful in that it serves
as a strong reminder to Federal managers on the importance
of security measures for ADP facilities.

There is no question that Federal managers have a responsi-
bility for protecting automatic data processing equipment and
the associated software, as well as the data processed on
this equipment from unauthorized use, acts of destruction,
alteration or misuse.  However, catastrophic losses to
Federal data processing installations caused by flood, fire,
explosions, etc. can never be completely eliminated.  As
stated in the report, "Perfect security is generally regarded
as unattainable; therefore, the aim of a good physical
security system should be to reduce the probability of loss
to an acceptable low level of reasonable costs and to ensure
adequate recovery in case of loss."  We strongly support
this concept of risk management.

It is our view that computer security should be viewed in
the broader context of protecting agency installations,
operations and records from a variety of potential threats
and hazards and should not be treated separately.  The
head of each agency is already responsible for (1) assuring
that the resources of his or her agency are properly pro-
tected (and necessary emergency back-up facilities and
or services are available) to assure continued operation
of critical agency activities; and (2) establishing whatever
safeguards are appropriate to protect against threats to
agency security.  In the latter area, the concept of risk

50

management outlined in the Appendix I of your report has
particular utility.  Assistance and policy guidance is
available to the agency from the Civil Service Commission
(for personnel security) and from the General Services
Administration (for building security and continuity of
operations).  Also, each major agency currently has a
Security Officer whose responsibilities include personnel
security as well as coordination with GSA on aspects of
physical security within the building.  We believe the
agency head should be responsible for determining both
the measures that are necessary, as well as how to
organize to assure effective security; and question the
appropriateness of directing that a separate official be
named for ADP security.

Your report was generally supportive of the National
Bureau of Standards guidelines on ADP physical security
and risk management, but also indicated that improvements
should be made in the guidelines.

We question whether it is necessary for OMB to issue any
further policy directives at this time regarding application
and use of the NBS guidelines.  The responsibility and
authority for developing, coordinating and issuing appro-
priate uniform ADP standards under the authority of
P.L. 89-306 was delegated to the Secretary of Commerce
by Executive Order 11717 dated May 9, 1973.  The authority
for developing any additional computer and data security
standards that may be required to meet the requirements
of the Privacy Act of 1974 (P.L. 93-579) were assigned
to the Secretary of Commerce under OMB Circular No. A-108
dated July 1, 1975.  While OMB recognizes and accepts
its responsibility for policy formulation and oversight
in these areas, we believe it would be more appropriate
to direct specific recommendations on the improvement
and strengthening of the existing guidelines and their
use to the National Bureau of Standards of the Department
of Commerce since they are the government's functional
experts for this subject.

We share the view, implicit in the report, that there is
a need for greater awareness of threats to physical
security (particularly in ADP) and suggest that your
final report address specific recommendations to those
agencies you found to be lacking in adequate security

safeguards. We would also encourage wide dissemination
of your report to each of the previously mentioned
functional groups so that all concerned are adequately
sensitized to this problem. We would be happy to assist
in assuring that appropriate organizational elements
within various agencies are made aware of the findings
and conclusions of the final report.

We will continue to be supportive of the objective of
this report and where appropriate will reflect ADP
security requirements in OMB policies.

Sincerely yours,
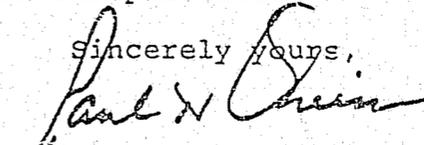
James T. Lynn
Director

UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Administration
Washington, D.C. 20230

17 MAR 1976

Mr. Victor L. Lowe
Director, General Government Division
U. S. General Accounting Office
Washington, D. C. 20548

Dear Mr. Lowe:

This is in reply to your letter of February 11, 1976,
requesting comments on the draft report entitled "Federal
Managers Need to Provide Better Protection for Automatic
Data Processing Facilities."

We have reviewed the enclosed comments of the Assistant
Secretary for Science and Technology and believe they
are responsive to the matters discussed in the report.

Sincerely,
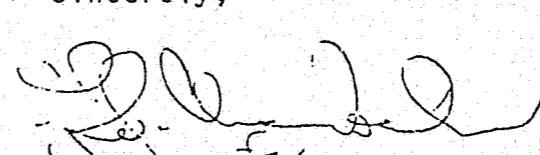
Joseph E. Kasputys
Assistant Secretary
   for Administration

Enclosure
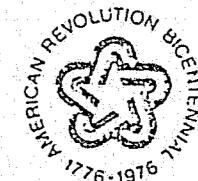
53

UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Science and Technology
Washington, D.C. 20230

Mr. Victor L. Lowe
Director, General Government Division
U.S. General Accounting Office
Washington, D.C.  20548

Dear Mr. Lowe:

The GAO draft report, "Federal Managers Need to Provide Better
Protection for Automatic Data Processing Facilities", sent to
the Secretary for comment, contains numerous references to the
National Bureau of Standards (NBS) publication "Guidelines for
Automatic Data Processing Physical Security and Risk Management."
In the large, the draft report is quite complimentary to the NBS
guidelines.  We are glad to have provided a vehicle which is of
such importance to the Federal data processing community and would
certainly undertake considering the recommendations for changes in
the next edition of the guidelines.

One recommendation of the report is the appointment for each data
processing facility of a management official responsible for auto-
matic data processing (ADP) physical security and risk management.
Page 38 of the report indicates that this management official should
be outside of the ADP organization.  This is not entirely clear in the
recommendation.  We infer that the attendant structure to support this
person in all agency's substructures would also be necessary.  This,
coupled with the current requirement for privacy officers, represents
fairly significant efforts.  Consideration should be given to revising
the recommendation so that physical security responsibility be assigned
a person in the ADP organization with a physical security audit function
established external to the ADP organization.  This audit function
would ensure the consistency and adequacy of the safeguards and procedures.

Thank you for this opportunity to comment on the draft report.

Sincerely,

Betsy Ancker-Johnson, Ph.D.

54

ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

COMPTROLLER

15 MAR 1976

Mr. Donald L. Scantlebury
Director, Financial and General
   Management Studies Division
U.S. General Accounting Office
Washington, D.C.  20548

Dear Mr. Scantlebury:

The Secretary of Defense has asked me to respond to your
February 10, 1976 letter inviting comments on an enclosed
GAO proposed report "Federal Managers Need to Provide Better
Protection for Automatic Data Processing Facilities."  This
opportunity is appreciated and our comments follow hereafter.

The importance of the subject, the general substance of the
report, and the thrust of the recommendations are wholeheartedly
endorsed, subject to the following points:

   1.  The Digest on Page 1 refers to protection from
". . .unauthorized acts. . . ."  It should also include
"inadvertent acts."

   2.  The first recommendation pertaining to the appointment
of an ADP physical security and risk management official,
should explicitly call for him to be highly knowledgeable in
ADP, as well as apart from the direct management of the ADP
facility.  This is required so as to provide the technical
skill needed to recognize vulnerabilities while avoiding possible
conflicts of interest.

   3.  The second recommendation should not require the NBS
guidelines to be mandatory at this time.  Their use as
"Guidelines" rather than "Standards" was specifically selected
after considerable deliberation by the Federal Information
Processing Standards Coordination and Advisory Committee (FIPSCAC)
in order to achieve an early dissemination of useful reference
information which was not yet sufficiently developed to the point
where they could undergo the more thorough coordination required
for a mandatory standard.  After further refinement, it is expected
to become a standard but that point of maturation has not yet
been reached.  Further, DoD Directive 5200.28, "Security Requirements

for ADP Systems," and DoD Manual 5200.28M, "ADP Security Manual," cover much of the same areas as the NBS guidelines. The substance of these documents, as well as documents from other agencies and industry, should be melded to provide a comprehensive set of concepts and guidelines for use of the government agencies in developing their respective policies.

I appreciate this opportunity to comment.

Sincerely,
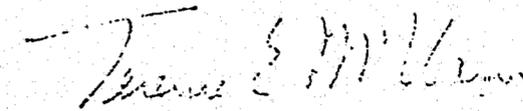
Terence E. McClary
Assistant Secretary of Defense

DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE
OFFICE OF THE SECRETARY
WASHINGTON, D C.  20201

MAR 15 1976

Mr. Gregory J. Ahart
Director, Manpower and
  Welfare Division
United States General
  Accounting Office
Washington, D.C.  20548

Dear Mr. Ahart:

The Secretary asked that I respond to your request for
our comments on your draft report entitled, "Federal
Managers Need to Provide Better Protection for Automated
Data Processing Facilities."

We fully concur with the recommendations contained in
the report (appc     ent of a management official respon-
sible for ADP ph  .cal security and risk management, and
establishment of policy dictating the use of NBS guide-
lines in those programs).  In fact, this Department
issued ADP Standards for ADP Systems Security in July
1975 which contain exactly these requirements.

We appreciate the opportunity to comment on this draft
report before its publication.

Sincerely yours,
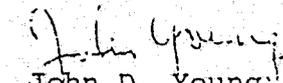
John D. Young
Assistant Secretary, Comptroller

57

OFFICE OF THE SECRETARY OF TRANSPORTATION
WASHINGTON, D.C.  20590

ASSISTANT SECRETARY
FOR ADMINISTRATION

March 12, 1976

Mr. Donald Scantlebury
Director
Financial and General Management
  Studies Division
U. S. General Accounting Office
Washington, D. C.  20548

Dear Mr. Scantlebury:

We have reviewed the draft report entitled "Federal Managers Need to
Provide Better Protection for Automatic Data Processing Facilities."
The Department of Transportation concurs with the draft report and
the recommendations to designate a management official to be
responsible for ADP physical security at each processing facility
and to use the National Bureau of Standards' guidelines.

Editorially, we request that the reference to the "Federal Aviation
Agency" on page 1 be changed to read "Federal Aviation Administration."
Also, the reference to Public Law 93-597 on page 6 appears to mean the
Privacy Act of 1974 which is Public Law 93-579.

Sincerely,
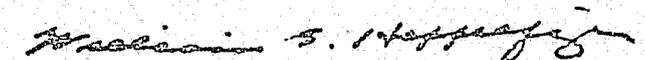
William S. Heffelfinger

Federal Information
Processing Standards Publication 31

1974 June

ANNOUNCING THE

## GUIDELINES FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT

### Action Summary

The essential recommendat . . . his publication are summarized here to show the scope of these guidelines and . . . ide a quick overview of action items in establishing, implementing and maintaining . physical security program in an ADP facility.

I. Organize The ADP Physical Security P· gram

Assign responsibility for ADP Physical Security and establish a task force to prepare a plan for the ADP security program.

Perform a preliminary risk analysis to identify major problem areas and select interim security measures as needed to correct major problem areas.

II. Conduct A Risk Analysis

Estimate potential losses to the ADP facility and its users from (1) physical destruction or theft of physical assets; (2) loss or destruction of data and program files; (?) theft of information; (4) theft of indirect assets; and (5) delay or prevention of computer processing.

Estimate the probability of occurrence for potential threats and their effect on the ADP facility in terms of the five classes of loss potential.
Combine the estimates of loss potential and threat probability to develop an annual loss expectancy.

Select the array of remedial measures which effects the greatest reduction in the annual loss expectancy at the least total cost. Remedial measures will include: (1) changes in the environment to reduce exposure; (2) measures to reduce the effect of a threat; (3) improved control procedures; (4) early detection; and (5) contingency plans.

III. Determine Local Natural Disaster Probabilities

Evaluate the fire safety of the ADP facility (building location, construction, occupancy and housekeeping) and provide required fire detection and extinguishment, and possibly a trained fire fighting brigade.

Evaluate the exposure to flooding from internal and external sources. Where needed, provide flood protection for the building relocate ADP hardware, reroute plumbing lines and provide water damage/flood-control equipment (pumps, tarpaulins, etc.)
Evaluate resistance of the building to wind and water damage if exposed to hurricanes, tornadoes or other high winds.

IV. Initiate A Security Program

Prepare a plan and a schedule for implementing selected remedial measures.
Prepare and maintain a policy and plans handbook to include: (1) an ADP physical
security policy statement; (2) mandatory security procedures; (3) security guidelines
for system design, programming, testing, and maintenance; (4) contingency plans;
(5) security indoctrination materials; and (6) a security audit program.

V. Protect Supporting Utilities

Estimate the number and duration of electric power transients, undervoltage condi-
tions and power interruptions and their annual loss expectancy. Install appropriate
protective equipment such as: voltage regulating transformers, dual power feeders,
uninterruptible power supplies, on-site power generators and ADP power isolation
circuits.

Estimate annual loss expectancy from air conditioning failures considering required
operation schedules, annual profiles of local temperature and humidity, and an esti-
mated number and duration of air conditioning failures. Where necessary, increase
reliability with redundant equipment, provide for emergency use of outside air and
augment maintenance capability to decrease mean time to repair.

Estimate the annual loss expectancy from teleprocessing circuit failures. Where cost is
justified, increase reliability with redundant communications circuits and augment repair
facilities to decrease the duration of interruptions. Software should be designed to min-
imize the impact of errors caused by communications failures.

Determine if ADP operations could be interrupted by the failure of other supporting
utilities such as water, natural gas, steam, elevators or mail conveyors. If necessary,
take steps to increase reliability and decrease the mean time to repair.

VI. Optimize Computer Reliability

Perform a failure analysis to estimate the number and duration of significant hard-
ware failures and their impact on ADP operations. Estimate the annual loss expectancy
from delays in performing urgent ADP tasks. Where cost is justified, increase system
reliability by adding peripherals, multiple configurations, etc. Review maintenance fa-
cilities. Record and analyze all hardware failures in order to identify failure trends
promptly and optimize preventive maintenance.

VII. Provide Physical Protection

Identify critical ADP areas including the computer room, data control and conversion
area, data file storage area, programmer's area, forms storage area, maintenance area,
and mechanical equipment room, and then provide adequate physical protection and
access control.

Protect against theft, vandalism, sabotage, espionage, civil disorder and other forced
intrusions with improved lighting and intrusion detection systems, with physical bar-
riers at doors, windows, and other openings, and with guards as required.

Control access to critical areas and ADP facilities with conventional or electronic door
locks; supervision by guards or receptionists over movement of people and materials;
administrative procedures (sign-in logs, identification cards or badges, property passes
and shipping/receiving forms); and other regulations.

VIII. Add Internal Procedural Security

Determine potential targets for fraud, theft or misuse of resources by analyzing the
work flow and the nature of ADP tasks performed. Incorporate procedures which will
minimize exposure to loss. Such procedures may include (1) requiring cooperation be-
tween two individuals to perform critical tasks; (2) performing additional checks and
bounds comparisons; (3) formalizing standards for high risk operations; and (4) in-
dependent quality control checks.

Designate critical positions in ADP management, system programming, program library control, input/output control, exception processing, applications programming, data base management, quality control, internal audit and hardware maintenance and require appropriate pre-employment screening.

Train and supervise all ADP personnel to assure understanding of, and compliance with, internal controls.

Implement control and record keeping procedures for job initiation, scheduling and distribution of output to prevent unauthorized processing.

Control access to physical data files to assure that data integrity is maintained, storage media are protected, custody of data files is traceable and their unauthorized use is prevented. Manual and automatic audit trails should be utilized.

Establish policy and procedures for program and data file retention to satisfy requirements for (1) back-up operation; (2) compliance with applicable statutes and regulation; (3) audit and management review of operation; (4) statistical analysis of operations; and (5) resolution of data integrity problems.

Implement programming, testing and documentation standards which satisfy requirements for (1) audit capability; (2) automated acceptance testing; (3) control program maintenance; (4) quality controls on input data; and (5) non-dependence on an individual's knowledge of systems and programs.

## IX. Plan For Contingencies

Compile a set of back-up plans which accommodate the expected range of emergency events requiring back-up operation. The objective of such contingency plans is to protect users of the ADP facility against unacceptable loss. Document performance specifications, operation instructions and technical requirements (system hardware and software, program and data files, and preprinted forms) for each emergency operation

Select and periodically use an emergency back-up off-site ADP facility. Participate in establishing their security program.

Provide protection for the source documents, input and output data and programs while using the off-site facility and in transit.

Establish procedures to assure that (1) current copies of needed back-up materials are retained at a secure off-site location; (2) adequate time is available from compatible off-site ADP facilities; and (3) back-up personnel will be available if needed.

Plan for reconstruction of the ADP facility following destruction including specifications of (1) floor space (quantity, live load rating, location, etc. by functional use) ; (2) partitions, electr. power service, air conditioning, communications, security, fire safety, etc.; and (3) ADP hardware, office equipment and supplies.

Coordinate ADP emergency plans for fire, flood, civil disorders, etc. with the Facility Self-Protection Plan to ensure life safety, limit damage, minimize disruption to ADP operations, and expedite repair.

## X. Develop Security Awareness

Determine the security training requirements for the ADP staff, senior management, building staff, etc.

Select and implement appropriate security awareness techniques such as (1) training lectures and seminars; (2) posters; (3) orientation booklets; (4) amendments to job descriptions making employees responsible for security; (5) publicity for local security incidents, as well as others occurring at similar installations; and (6) rewards for employees who prevent breeches in security.

Establish and publicize punitive measures.

XI. Audit Physical Security

Establish an internal audit team with representatives from the agency's audit, building safety and security, ADP, and users' organizations.

Develop an audit plan and schedule which systematically validates all critical security and emergency measures.

State in the audit report which measures require improvement or replacement. Use a check sheet (problem description, responsibility for action, action required and follow-up) for each major deficiency to assure prompt resolution.

END