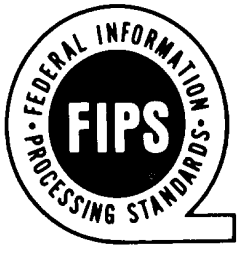
FIPS PUB 41

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1975 MAY 30

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards



COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

CATEGORY: ADP OPERATIONS

SUBCATEGORY: COMPUTER SECURITY

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89–306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of government efforts in the development of technical guidelines and standards in these areas.

The selective application of technological and related procedural safeguards is an important component of the Federal Government's efforts to protect the privacy of individuals, as required by the Privacy Act of 1974. The guidelines provided by this publication establish the groundwork for assessing the risks of unauthorized disclosures of personal data in current automated systems and developing a set of safeguards to minimize those risks. They are made available for use by Federal agencies within the context of the Office of Management and Budget's total program for implementing the Privacy Act.

RUTH M. DAVIS, Director
Institute for Computer Sciences
and Technology

Abstract

This publication provides guidelines for use by Federal ADP organizations in implementing the computer security safeguards necessary for compliance with Public Law 93–579, the Privacy Act of 1974. A wide variety of technical and related procedural safeguards are described. These fall into three broad categories: Physical security, information management practices, and computer system/network security controls. As each organization processing personal data has unique characteristics, specific organizations should draw upon the material provided in order to select a well-balanced combination of safeguards which meets their particular requirements.

Key words: Access controls; ADP security; computer security; Federal Information Processing Standards; information management; personal data; physical security; privacy risk assessment.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 41, 20 pages, (1975) CODEN: FIPPAT

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. (Order by SD Catalog No. C13.52:41). GPO price 70 cents.

Federal Information Processing Standards Publication 41

1975 May 30

ANNOUNCING THE

COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 CFR (Code of Federal Regulations).

Name of Guideline: Computer Security Guidelines for Implementing the Privacy Act of 1974.

Category of Guideline: ADP Operations, Computer Security.

Explanation: The Privacy Act of 1974 imposes numerous requirements upon Federal agencies, to prevent the misuse or compromise of data concerning individuals. Federal ADP organizations which process personal data must provide a reasonable degree of protection against unauthorized disclosure, destruction or modification of personal data, whether intentionally caused or resulting from accident or carelessness. These guidelines provide a handbook for use by Federal organizations in implementing any computer security safeguards which they must adopt in order to implement the Act. They describe risks and risk assessment, physical security measures, appropriate information management practices, and computer system/network security controls.

Approving Authority. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency. Department of Commerce, National Bureau of Standards (Institute of Computer Sciences and Technology).

Cross Index. See Appendix.

Applicability. These guidelines were prepared at the specific request of the Office of Management and Budget and are intended for use in implementing the computer security requirements imposed by the Privacy Act of 1974. As they treat the general problem of computer security in addressing a host of available safeguards, they are also generally applicable to computer security matters unrelated to individual privacy.

Implementation. Each Federal ADP organization has unique requirements for computer security stemming from the Privacy Act of 1974. Specific needs depend on the organization's personal data processing mission and its operating environment. Utilizing the description of a wide variety of safeguards contained in these guidelines, an organization may select a well-balanced set which meets its particular needs.

Specifications. Federal Information Processing Standard 41 (FIPS 41), Computer Security Guidelines for Implementing the Privacy Act of 1974, (affixed).

Qualifications. This document provides a set of guidelines from which a Federal organization may select technical and related procedural safeguards for protecting personal data in automated information systems. It does not cover topics such as determination of the need for maintaining personal data and the relevance of the data to the performance of authorized functions. Also, matters such as employee rules of conduct, employee screening and training are outside the purview of this document.

As each organization has a unique set of requirements and risks to consider, depending on its environment, function and operations, no list of required safeguards can be prescribed in general. Each organization must analyze its own requirements. Computer security is only one facet of implementation of the Privacy Act of 1974, and this document therefore should be considered in conjunction with other issuances of the Office of Management and Budget, the General Services Administration, and the Civil Service Commission.

As new knowledge, techniques and devices become available in the future, these guidelines will need to be modified accordingly. Because of the new requirements of the Privacy Act of 1974 and anticipated technical and related procedural experiences, much information relevant to these guidelines will be gained. All comments and critiques are welcome, and will be considered in future revision. They should be addressed to the Systems and Software Division, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

Where to Obtain Copies of the Standard.

a. Copies of this publication are available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (SD Catalog Number C13.52:41). There is a 25 percent discount on quantities of 100 or more. When ordering, specify document number, title, and SD Catalog Number. Payment may be made by check, money order, coupons, or deposit account.

b. Microfiche of this publication is available from the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22151. When ordering refer to Report Number NBS–FIPS–PUB–41 and title. Payment may be made by check, money order, or deposit account.

Executive Overview

The Privacy Act of 1974 (5 U.S.C. 552a) imposes numerous requirements upon Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. These requirements will be met by the application of selected managerial, administrative and technical procedures which, in combination, can be used to achieve the objectives of the Act.

This document provides a set of guidelines for the use of technical procedures for safeguarding personal data in automated information systems. Managerial and administrative procedures such as those relating to basic determinations concerning the need for maintaining personal data and its relevance to the performance of authorized functions, employee rules of conduct, and employee screening and training are outside the purview of this document. The guidelines were prepared in response to the Office of Management and Budget memorandum dated March 12, 1975, *Implementation of the Privacy Act of 1974*, and are made available for consideration and use by all Federal agencies in meeting the requirements of the Act. They represent, however, only one segment of the Government-wide guidance that is provided for in OMB's circular governing the implementation of the Act and should, therefore, be considered in conjunction with all other guidance on this subject.

There are three categories of technical safeguards which can be used to maintain the integrity of personal information and protect it from unauthorized use. These categories are: physical security procedures, information management practices and computer system/network security controls. The guidelines cover all three categories; neither category by itself is likely to offer protection against all risks of privacy violations. However, by carefully selecting appropriate components from among all three categories and packaging them into a well-balanced set of safeguards according to individual needs, the level of protection can usually be improved significantly at reasonable cost.

The relevance and utility of these technical procedures can be grasped quickly if they are viewed in the context of the Privacy Act of 1974. Figure 1, on page 2, identifies the principal provisions of the Act which involve the application of safeguards and shows how each of the three categories can contribute to the implementation of these provisions. The matrix illustrates graphically not only that the procedures can be used in combination to administer various provisions of the Act, but also that some safeguards can simultaneously contribute to satisfying more than one provision. Significantly, it also indicates that the preservation of data integrity and security in automated systems can be achieved in good measure by the prudent use of physical security and information management practices and is not necessarily dependent upon complex computer system/network controls.

The major provisions of the Privacy Act which most directly involve the use of computer system/network controls are: Subsection (b) of 5 U.S.C. Section 552a which limits the disclosure of personal information to authorized persons and agencies; Subsection (e)(5) which requires the maintenance of accurate, relevant, timely, and complete records; and Subsection (e)(10) which requires the use of safeguards to insure the security and integrity of records. Although the Act sets up legislative prohibitions against unauthorized disclosures, system/network controls are also needed to help assure that access to personal data is properly controlled and that intentional or accidental violations of security and integrity do not occur.

These controls include techniques for providing positive identification of the authorized user of the system and remote terminals, authenticating his right to have access to specific data in a system shared by others and preventing him from gaining access to data and/or programs to which he is not entitled, and, finally, providing a system of internal audits for monitoring compliance with the stipulated security requirements. In cases involving the automated transfer of personal data between terminals and a computer system or among systems, protection requirements might, on infrequent occasions, be judged sufficiently strong to warrant the use of data encryption techniques.

Thus, in addition to viewing the technological safeguards in terms of the provisions of the Privacy Act, it is useful also to view them in terms of the control points within a computer system/network where security risks occur and where appropriate safeguards can be applied. This perspective is provided in figure 2 on pages 4 & 5, which portrays the elements of a computer system/network, beginning with the off-line storage of data in machine-readable media (e.g., tapes and discs) and progressing through the many possible processing modes, including the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses again the value of physical security and information management practices as major adjuncts to the computer system/network security controls of the type described in the preceding paragraph.

In order to provide for consistency and effectiveness in applying protective measures, the National Bureau of Standards has identified the need for technical standards and guidelines in the following topical areas:

- Physical security
  - Risk management
  - Fire and other disasters
  - Physical protection
  - Contingency planning
- Information management
  - Data input, storage and handling
  - Record identification
  - Media control
  - Programming techniques for security
  - Software documentation
  - Data elements
- Computer system/network security controls
  - User identification
  - Terminal identification
  - Data access controls
  - Data encryption
  - Security auditing

Within these topical areas, the National Bureau of Standards has already provided the following guidelines which are available and can be obtained as indicated in the Appendix:

- Executive Guide to Computer Security
- Guidelines for ADP Physical Security and Risk Management

It is intended that the standards and guidelines identified above will be examined, developed and published using regular or expedited procedures that are consistent with meeting the needs and problems generated by experience gained in administering the Privacy Act. Meanwhile, the guidelines included in this document are intended as a statement of technical measures which managers should consider together with managerial and administrative procedures as they decide upon a balanced set of safeguards suitable to their specific operational needs and environments.

Inquiries and comments regarding the application of these guidelines should be directed to the Systems and Software Division, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234. (Telephone: Area Code 301–921–3861)

Federal Information Processing Standards Publication 41

1975 May 30

Specifications for

COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

Contents

	Page
Executive Overview	3
1. INTRODUCTION	7
1.1. The Privacy Act of 1974	7
1.2. Scope of Guidelines	7
1.3. Definitions	7
1.4. Safeguards	7
2. SECURITY RISK ASSESSMENT AND SAFEGUARD SELECTION	9
2.1. Security Risk Assessment	9
2.2. Categories of Security Risks	12
2.2.1. Accidents, Errors, and Omissions	12
2.2.2. Risks from Uncontrolled System Access	12
2.2.3. Risks from Authorized Users of Personal Data	13
2.2.4. Risks from the Physical Environment and from Malicious Destructive Acts	13
2.2.5. Risks from Deliberate Penetrations	13
2.3. Cost Considerations for Selecting Safeguards	13
3. PHYSICAL SECURITY	14
3.1. Entry Controls	15
3.2. Storage Protection	15
4. INFORMATION MANAGEMENT PRACTICES	15
4.1. Handling of Personal Data	16
4.2. Maintenance of Records to Trace the Disposition of Personal Data	16
4.3. Data Processing Practices	16
4.4. Programming Practices	17
4.5. Assignment of Responsibilities	17
4.6. Procedural Auditing	17
5. SYSTEMS SECURITY	17
5.1. Identification	17
5.2. System Access Controls	18
5.3. Access Auditing	18
5.4. Network Systems	18
5.5. Planning for Future ADP Systems	19
5.5.1. Internal Controls	19
5.5.2. Data Encryption	19

1. Introduction

1.1. The Privacy Act of 1974

The Privacy Act of 1974 imposes numerous requirements upon Federal agencies to prevent the misuse of data about individuals, respect its confidentiality and preserve its integrity. Federal agencies can meet these requirements by the application of selected managerial, administrative and technical procedures which, in combination, achieve the objectives of the Act.

The major provisions of the Privacy Act which most directly involve computer security are found in the following parts of 5 U.S.C. Section 552a:

- Subsection (b), which limits disclosure of personal information to authorized persons and agencies;
- Subsection (e)(5), which requires accuracy, relevance, timeliness and completeness of records;
- Subsection (e)(10), which requires the use of safeguards to insure the confidentiality and security of records.

Although the Act sets up legislative prohibitions against abuses, technical and related procedural safeguards are required in order to establish a reasonable confidence that compliance is indeed achieved. It is thus necessary to provide a reasonable degree of protection against unauthorized disclosure, destruction or modification of personal data, whether intentionally caused or resulting from accident or carelessness.

1.2. Scope of Guidelines

This document was prepared at the request of the Office of Management and Budget. It provides a set of guidelines specifying technical and related procedural methods for protecting personal data in automated information systems and should be read in conjunction with OMB's circular on the implementation of the Privacy Act. Managerial and administrative procedures such as those relating to basic determinations concerning the need for maintaining personal data and its relevance to the performance of authorized functions, employee rules of conduct, and employee screening and training are outside the purview of this document. These guidelines represent only one aspect of Government-wide implementation guidance. Like the National Bureau of Standards, the General Services Administration and the Civil Service Commission have issued guidelines dealing with specific topics, under direction of the Office of Management and Budget.

1.3. Definitions

The following terminology is used throughout this document in discussing the treatment of data:

- Confidentiality—A concept which applies to data. It is the status accorded to data which requires protection from unauthorized disclosure.
- Data Integrity—The state existing when data agrees with the source from which it is derived, and when it has not been either accidentally or maliciously altered, disclosed or destroyed.
- Data Security—The protection of data from accidental or intentional, but unauthorized, modification, destruction or disclosure.

Safeguards which provide data protection are grouped into three categories: physical security measures, information management practices, and computer system/network security controls. Specifically, these are:

- Physical Security Measures—Measures for protecting the physical assets of a system and related facilities against environmental hazards or deliberate actions.
- Information Management Practices—Procedures for collecting, validating, processing, controlling and distributing data.
- Computer System/Network Security Controls—Techniques available in the hardware and software of a computer system or network for controlling the processing of and access to data and other assets.

1.4. Safeguards

The relevance and utility of these technical safeguards can be grasped quickly if they are viewed in the context of the Privacy Act of 1974. Figure 1 identifies the principal provisions of the Privacy Act which involve the application of safeguards and shows how each of the three categories can contribute to the implementation of these provisions. The matrix also serves to illustrate graphically that adopting particular safeguards may help to satisfy more than one requirement of the Act. Significantly, it also indicates that protection of data in automated systems is not necessarily dependent upon complex computer system/network technology, but can be achieved in good measure by the prudent use of physical security measures and information management practices.

The safeguards discussed here are aimed specifically at precluding unauthorized access to personal data in computer systems, but most of

them, especially those in the areas of physical security and information management, are applicable to manual as well as automated systems. Most of them also provide protection for other kinds of data than personal. However, since the present emphasis is on personal data, "data" is synonymous with "personal data" in the remainder of this document.

Figure 1 relates technological safeguards to specific provisions of the Privacy Act. Alternatively, they may be viewed in relation to the control points within a computer system/network where security risks occur and where appropriate safeguards can be applied. This perspective is provided in figure 2 on pages 10 and 11, which shows the elements of a computer network, beginning with the offline storage of data in machine-readable media (e.g., tapes and disks) and progressing through the many possible processing modes, including the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses again the value of physical security measures and information management practices, in relation to computer system/network controls.

These guidelines cover the three categories of safeguards defined in Section 1.2. The consideration of one to the exclusion of the others is not likely to offer protection against all risks of privacy violations. However, by carefully selecting a well-balanced set of safeguards, the level of protection can usually be improved significantly at reasonable cost.

SAFEGUARDS	SECTION OF GUIDELINES	REQUIREMENTS / SUBSECTION OF 5 U.S.C. SECTION 552a	Control of Disclosures (b)	Accounting of Disclosures (c) (1)	Provide Access to Records (d)	Inclusion of Disputed Information (d) (4)	Use Relevant Data Only for Authorized Purposes (e) (1)	Maintain Accurate, Complete Records (e) (5), (6)	Insure Integrity, Security and Confidentiality of Records (e) (10)	Retention of Records; Archival Storage (l) (1)
Physical Security	3.0									
Entry Controls	3.1		X						X	
Storage Protection	3.2		X					X	X	X
Information Management Practices	4.0									
Handling of Data	4.1		X		X				X	X
Maintenance of Records	4.2		X	X					X	
Data Processing Practices	4.3		X	X		X	X	X	X	
Programming Practices	4.4		X	X		X	X	X	X	
Assignment of Responsibilities	4.5		X						X	X
Procedural Auditing	4.6		X	X		X		X	X	X
Systems Security	5.0									
Identification	5.1		X		X		X		X	
Access Controls	5.2		X		X		X	X	X	
Access Auditing	5.3		X	X	X		X		X	X
Data Encryption	5.5.2		X				X	X	X	X

FIGURE 1. *Technical safeguards applied to requirements of the Privacy Act of 1974.*

2. Security Risk Assessment and Safeguard Selection

The most important managerial actions a Federal agency must take initially are first, to make sure that any records which the agency maintains are necessary and relevant to the performance of a lawful agency function and second to restrict authorizations for access to personal data to a minimum. A fundamental principle underlying the Privacy Act is that information not maintained about an individual cannot be misused to his detriment. The elimination of non-essential information not only reduces the likelihood of harmful actions, but, by keeping record-keeping practices to a minimum, also eases the task of safeguarding the essential data.

The technical requirements of the Privacy Act for safeguarding the confidentiality, integrity, and security of personal data are less detailed and specific than some of the other requirements. The level of security needed to support privacy depends on the uses which are made of the records, the uses which others could make of the records if they are inadvertently or intentionally disclosed and the harm that might accrue to the individual. Furthermore, security needs are dependent on the environment in which the system of records operates. The determination of which security safeguards are needed to protect a given system must be made by personnel who are very familiar with the information maintained and with the administrative, technical, and physical environment in which the system operates.

2.1. Security Risk Assessment

The first step toward improving a system's security is to determine its security risks. A security risk assessment benefits an agency in three ways:

(1) It provides a basis for deciding whether additional security safeguards are needed.

(2) It ensures that additional security safeguards will help to counter all the serious security risks.

(3) It saves money that might have been wasted on safeguards which do not significantly lower the overall risks and exposures.

The goal of a risk assessment is to identify and prioritize those events which would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event and its probability of occurrence.

Section 2.2 identifies certain general risks and discusses general priorities. A risk assessment can be successful even though it only identifies the most serious risks without attempting to quantify degrees of risk; however, the degree of risk should be estimated in quantitative terms when possible. This provides a better basis for deciding what security safeguards are necessary and reasonable. It is sometimes possible to arrive at quantified estimates of risk which, though inexact, are still adequate for the purpose of selecting appropriate safeguards.

Estimates of the expected frequency of accidental risks can be based on previous experience of the agency and of other agencies with similar record systems. For risks that arise from deliberate acts, estimate the cost of carrying out the threat. Risks of deliberate penetration are far more likely when someone can benefit substantially from the act—especially when the act requires little effort or knowledge on his part. An operator with free access to the agency's ADP center may browse through sensitive files at virtually no cost to himself, whereas an individual intent on the unlikely act of undetectable interception of computer transmissions may require major capital and operating investments.

• In general the risk assessment should consider all risks—not just risks to personal data. While these guidelines emphasize the security of personal data, it is best to develop an integrated set of security safeguards which protest all valuable data on the system wherever possible.

The risk assessment should be conducted by a team which is fully familiar with the problems that occur in the daily handling and processing of the information. The participants on the risk assessment team should include experienced representatives from:

(1) the operating unit supported by or having jurisdiction over the data under consideration,

(2) the programmers responsible for support of the operation or function under consideration.

(3) the unit responsible for managing ADP operations,

(4) the system programmers—if the agency has this as a separate function,

(5) the person assigned the responsibility for overseeing or auditing system security.

(6) those responsible for physical security.

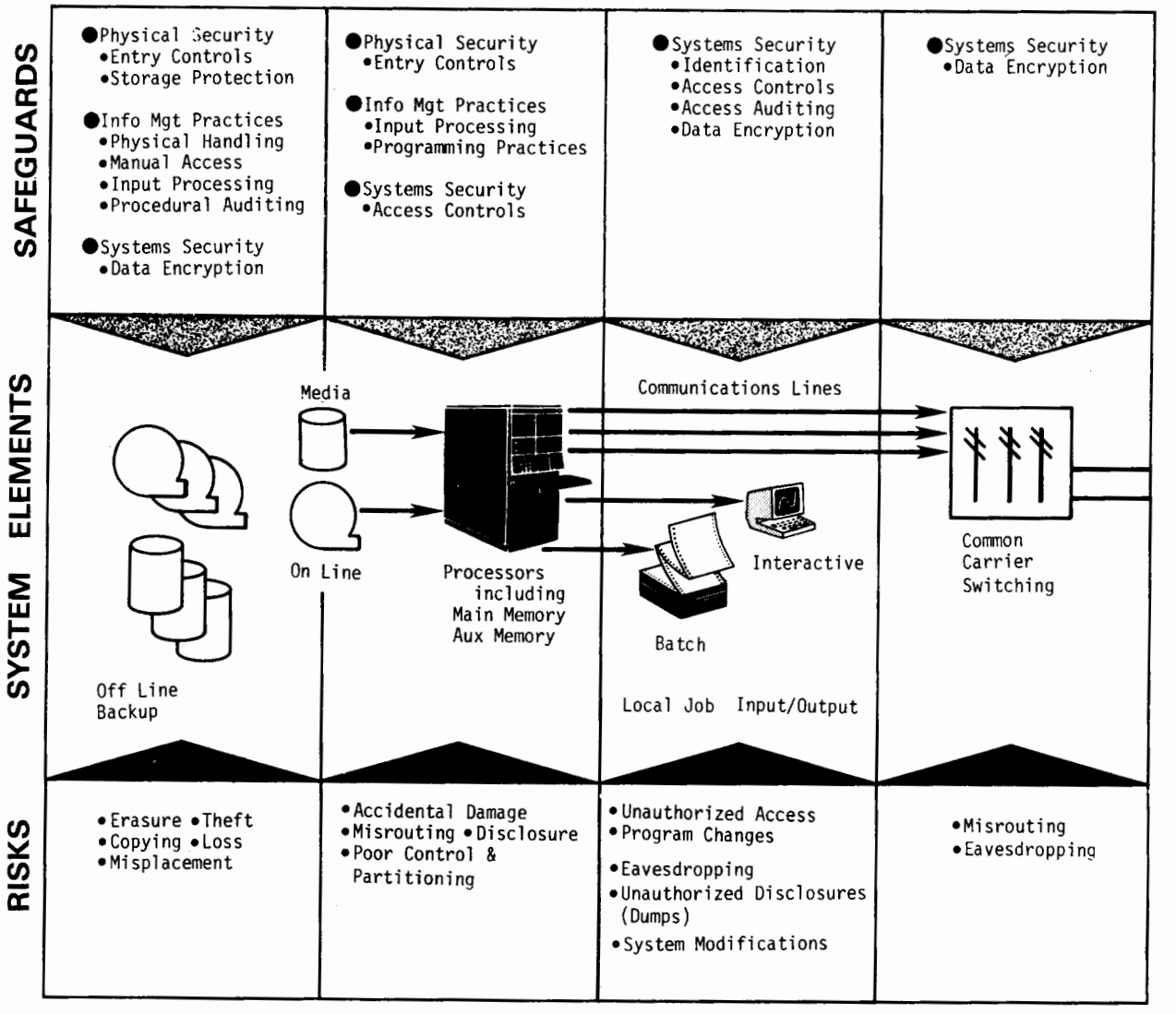
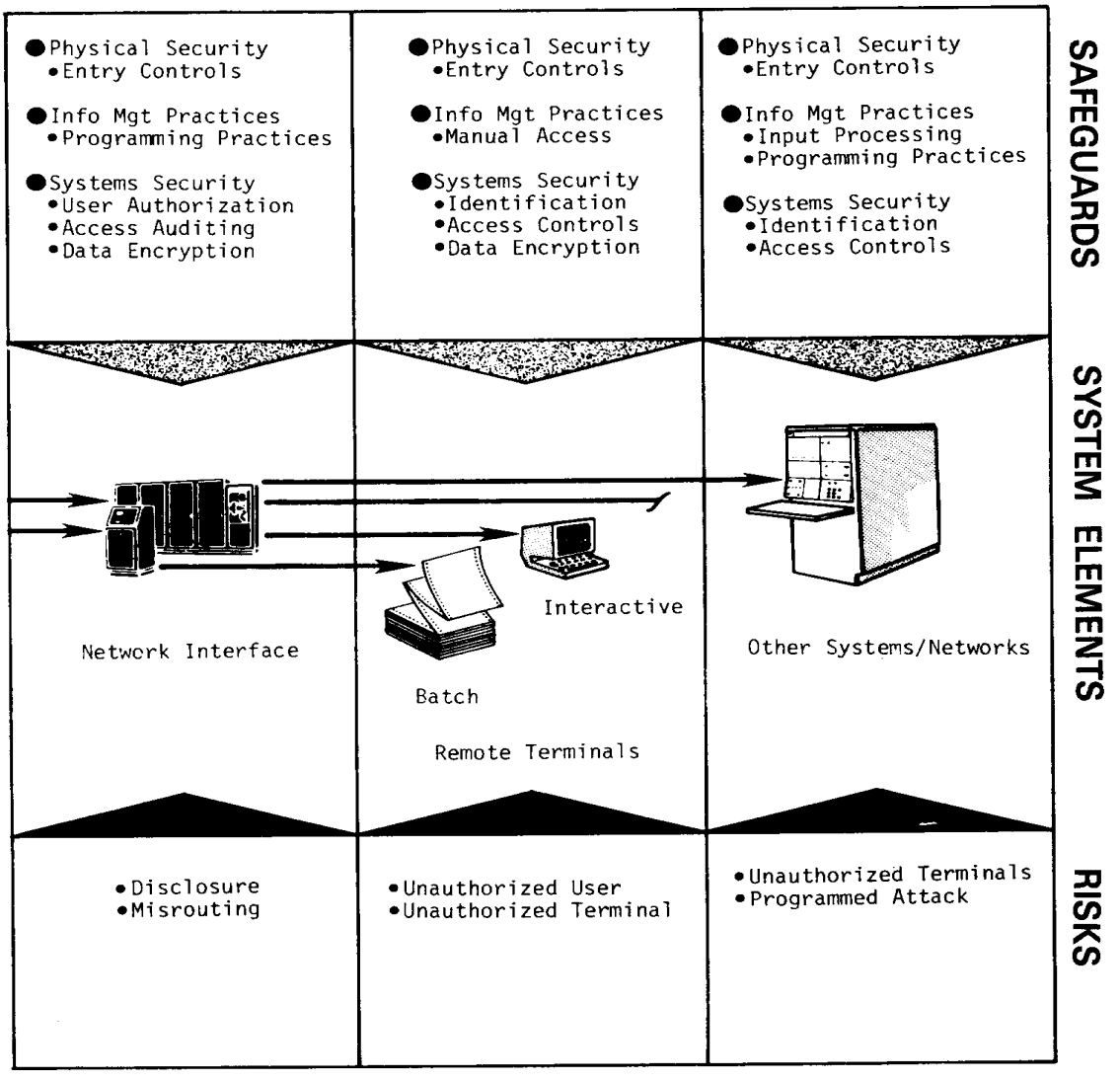


FIGURE 2. *Technical safeguards and data security risks.*



2.2. Categories of Security Risks

In this section general classes of security risks are identified and categorized as an initial illustration of risk assessment and as a step toward understanding the scope of security concerns. Risks must be assessed with respect to every file of personal information in the system. Each agency will have to identify its specific risks and evaluate the impact of those risks in terms of its information files.

The risks listed in the following subsections progress from acts of carelessness to system penetrations requiring significant technical sophistication. Risks are generally listed in the order in which they are likely to be encountered; however, each agency must realize that its risks could be prioritized differently if unique circumstances exist. Those agencies designing new ADP systems—especially large, remote-access systems—should consider the risks of deliberate system penetration at the time they are initially determining the system configuration.

2.2.1. Accidents, Errors, and Omissions

Experience indicates that the most commonly encountered security risks are usually accidents, errors and omissions. The damage from these accidental events far exceeds the damage from all other security risks. Good information management practices are necessary to reduce the damage that can result from these occurrences.

Some examples of these risks are:

- Input error—Data may not be checked for consistency and reasonableness at the time they are entered into the system; or data may be disclosed, modified, lost, or misidentified during input processing.
- Program errors—Programs can contain many undetected errors—especially when they are written with poor programming practices or are not extensively tested. A program error may result in undesirable modification, disclosure or destruction of sensitive information.
- Mistaken processing of data—Processing requests may update the wrong data; for example, if a tape is mounted at the wrong time.
- Data loss—Data on paper printouts, magnetic tapes, or other removable storage media may be lost, misplaced, or destroyed.
- Improper data dissemination—Disseminated data may be misrouted or mislabeled, or it may contain unexpected personal information.
- Careless disposal—Personal data can be retrieved from waste paper baskets, magnetic tapes, or discarded files.

2.2.2. Risks from Uncontrolled System Access

Agencies expose themselves to unnecessary risks if they fail to establish controls over who can access the personal data which is processed on their ADP systems. Outsiders must not have free access to the personal data. The number of agency employees with access to personal data must also be kept as small as possible without hindering the mission of the agency.

Physical security measures are always needed to control system access. If everyone using the ADP system is authorized access to all the personal data being processed, then physical security measures can adequately control system access. If the system is also used by some who should not be authorized access to all types of personal data, then information handling practices and system access controls are also needed to control these risks.

Examples of these risks include:

- Open system access—There may be no control over who can either use the ADP system or enter the computer room.
- Theft of data—Personal data may be stolen from the computer room or other places where it is stored.
- Unprotected files—Data files may not be protected from unauthorized access by other users of the ADP system. This applies to on-line files and also to off-line files such as magnetic tapes. The latter are sometimes accessible simply by requesting that they be mounted.
- Dial-in access—There is serious danger that unauthorized persons can access the system when remote, dial-in access is allowed.
- Open access during abnormal circumstances—Data which is adequately protected during normal operations may not be adequately protected under abnormal circumstances. Abnormal circumstances, include power failures, bomb threats, and natural disasters such as fire or flood.

2.2.3. Risks from Authorized Users of Personal Data

Experience with computer-related crime indicates that the most serious risks from deliberate acts are from employees who work with the data. These employees often know exactly what security safeguards are in effect, and they may know how to get around them as well. Protection of personal data from abuse by those authorized to access it is an important security concern.

Practices which contribute to these risks include:

- Poorly defined criteria for authorized access—Personnel may not know whether another employee should have access to a data item.
- Lax attitude toward employee dishonesty—Employee dishonesty may be relatively common and tolerated by management. Rules of conduct for agency employees having access to personal data must be established.
- Unaudited access to personal data—If an individual can access personal data knowing that there is no audit trail recording his access, then he will feel he cannot be held accountable for that act.

2.2.4. Risks from the Physical Environment and from Malicious Destructive Acts

Physical destruction or disabling of the ADP system is not usually a primary risk to privacy. Environmental hazards and malicious acts may destroy records required by the Privacy Act, or they may damage the accuracy, timeliness, or completeness of records. However, these risks are also serious because of the value of the resources that might be destroyed and because the agency's mission is often dependent on records in the ADP system. Security safeguards—including file back-up and contingency planning—needed and usually provided for these other reasons will normally be more than adequate to protect privacy against these risks.

Examples of these risks include:

- Fire, heat, water damage, and flood
- Electric power failure
- Malicious destruction by employees or outsiders.

2.2.5. Risks from Deliberate Penetrations

Current computer systems are vulnerable to deliberate penetrations, which can bypass routine security controls. These penetrations usually require the participation of an individual with specific technical knowledge. To date, there have been relatively few instances of substantial harm resulting from such deliberate penetrations. Thus these risks now appear to be less likely than most of the other risks mentioned above. The knowledgeable penetrator usually acts rationally, and the personal data would have to be very valuable to be attractive to him. However, agencies should be aware that attackers may try to embarrass the agency by demonstrating that their personal data is not secure.

In the future, risks from deliberate penetrations could become more significant. These potential risks will be greatly magnified by large computer networks. Agencies that are designing such networks for future use should consider these risks in the early planning stage.

Deliberate penetration risks include:

- Misidentified access—Passwords are often used to control access to a computer or to data, but they are notoriously easy to obtain if their use is not carefully controlled. Furthermore, a person may use an already logged-in terminal which the authorized user has left unattended, or he may capture a communications port as an authorized user attempts to disconnect from it.
- Operating system flaws—Design and implementation errors in operating systems allow a user to gain control of the system. Once the user is in control, he can disable auditing controls, erase audit trails, and access any information on the system.
- Subverting programs—Programs containing hidden subprograms that disable security protections can be submitted. Other programs can copy personal files into secret or misidentified files to use when protection is relaxed.
- Spoofing—Actions can be taken to mislead system personnel or the system software into performing an operation that appears normal but actually results in unauthorized access.
- Eavesdropping—Communications lines can be "monitored" by unauthorized terminals to obtain or modify information or to gain unauthorized access to an ADP system.

2.3. Cost Considerations for Selecting Safeguards

Each agency should consider the cost of each safeguard when selecting from among the several options available. While each agency must consider its own unique circumstances in assess-

ing costs, general guidelines for understanding cost parameters will assist in developing priorities for action.

Costs fall into two major areas: initial and operating costs. Initial costs include the purchase of new system elements, modification of existing systems to accept the new element, one-time administrative measures to support the new elements, and the initial testing of their effectiveness. Operating costs include the increased day-to-day costs of running the enhanced system, including such cost components as personnel, computer processing, storage, and system monitoring.

Security is needed as a prerequisite to privacy, but it is also needed for many other reasons. Basic security safeguards adequate to protect other valuable data such as financial and payroll records may also be adequate to support privacy. Only a small fraction of overall computer security costs is likely to be attributable to privacy. Agencies should wherever feasible keep the costs of security measures installed for other reasons separate from the costs of assuring privacy.

A risk assessment will have identified those risks which need to be controlled. Sections 3, 4, and 5 discuss various security controls which can be used. When these protection mechanisms are selected they should constitute a system of complementary measures that provide protection where it is needed. Each protective measure should be assessed in terms of the *incremental* protection achieved by the additional cost. A small amount spent for protection may increase the cost of intentional damage beyond an acceptable limit. A lock on a tape cabinet may provide all the protection needed for certain files since the simple lock raises an act of unauthorized access to one of "breaking-in." On the other hand, it would provide little protection against an irrational act of vandalism.

Physical security should be reviewed first, and improved where necessary. For most agencies, the application of physical security measures provides sufficient protection against intentional or overt external acts against agency data. However, it provides little protection against accidental or unintentional damage to files or against overt internal acts. Appropriate *information management practices* will provide a significant level of protection against many risks not covered by physical security. *System security safeguards* should be considered by those agencies whose data sensitivity levels require more protection than that offered by physical security and information management practices.

3. Physical Security

Physical security as it pertains to the protection of data does not differ from physical security for protecting other resources. It is achieved through the use of locks, guards, and administratively controlled procedures as well as measures required for the protection of the structures housing the computer and related equipment against damage from accident, fire and environmental hazard, thus ensuring the protection of their contents. Extensive guidelines for assessing physical security risks and applying appropriate measures are provided in *Guidelines for Automatic Data Processing Physical Security and Risk Management* (see Appendix). This section highlights considerations for determining the need for and application of physical security measures.

Security at an entrance to a computer center can prevent entry by all but the most determined intruders. Prevention of unauthorized entry into a facility can be accomplished not only by establishing a guard force but also by controlling all possible means of access from the exterior, including even such remote avenues as air conditioning vents, and through the use of sign-in procedures, badges for authorized personnel, special locks, exterior lighting, TV cameras, barriers (fences), and intrusion detection devices.

A thorough survey of the environment of a facility will disclose any special dangers in the area such as chemical or explosives activity or likelihood of flood, improper storage of combustibles, inadequate visitor control and other obvious hazards which could result in situations where data might be destroyed or exposed to public scrutiny or haphazard removal. In fact, such obvious perils should be considered before selecting the location for a computer facility although they are sometimes unavoidable.

It is reasonable to assume that protection against fire, explosion and natural disasters will be available in any computer installation, but additional measures may be necessary to insure the confidentiality and security of records. The risks to data which can be generated by a disaster situation stem not only from the vulnerability of the data's storage medium to destruction occurring during the actual catastrophe but extend to subsequent exposure of the media, reports and source materials in a damaged facility. In a disaster, accidental or not, risks to stored data also include damage caused by weather, firefighting techniques, salvage operations, vandalism, or theft.

While no hard and fast rules exist to determine the need or extent of physical protection measures for a given situation, a number of possibilities exist that should be considered. For any specific installation, some set of the measures described below must be selected for implementation in order to provide adequate safeguards against the unauthorized destruction, disclosure or modification of personal data.

3.1. Entry Controls

- Limit the number of entrances to the computer facility to a minimum. (There should be coordination of this measure with those responsible for fire protection and building security.) Doors should be of sufficient strength to resist forced entry.
- Install a screening device at every entrance, be it a guard, a badge reader, an electronic lock, a TV camera manned by a guard in another location, or a physical lock. Maintain entry logs wherever possible. Monitor closely all items moving into or out of the facility, whether expected or not, e.g., a scheduled delivery.
- If there is an extensive perimeter requiring protection, consider use of exterior lighting, TV cameras, roving patrols, intrusion detection devices; however, such protection is usually not the responsibility of the ADP manager.
- Secure all openings through which an intruder could gain entrance or receive material.
- Control the use of badges to permit entry. They should not be issued in such quantity that guards cannot verify badge holders. When people leave the employ of the facility, whatever the reason, it is essential to retrieve all keys, badges, etc., which have been issued to them. Visitors should be issued temporary badges differing in appearance from employee badges.
- In case of any unusual diversions such as power outages, bomb threats, false fire alarms, make a thorough search of the facility to prevent or to uncover loss or destructive activity which might have taken place during any confusion. Entry logs or other records of facility activity should be consulted; they might reveal any unusual occurrence that could serve as a clue to the identity of the perpetrator of the event.
- Provide adequate protection for remote terminals, tape libraries, trash areas, etc., which are not within the confines of the computer facility.

3.2. Storage Protection

- Devise fire protection plans with data storage media in mind. Consider the risks which firefighting imposes on stored data. Tape and disk library vaults (safes) can be certified to have a particular protection rating and design which keeps contents safe from steam and water damage as well as from heat and flame. These ratings should be considered in evaluating and selecting storage facilities.
- Include protective measures in planning for disaster response. Disaster recovery procedures should be periodically tested and exercised. Arrangements should be made for the removal to a place of safekeeping of storage media, computer printouts, records of disclosure and source material. If potential threats of looting and pilfering exist, guards should be posted; if data is vulnerable to water damage, protective plastic covers should be available.
- To ensure that protection of data is adequately maintained, conduct frequent unscheduled security inspections. Check for unlocked doors, doors propped open, locks which do not latch, and fire and intrusion alarms which have been turned off because they are too easily activated.

Physical security measures are the first line of defense against the risks which stem from the uncertainties in the environment as well as from the unpredictability of human behavior. Frequently, they are the simplest safeguards to implement and can be put into practice with the least delay. Naturally, not all physical security measures are required at any one installation, but rather a judicious selection which provides a realistic overall coverage for the lowest expenditure.

4. Information Management Practices

Information management practices refer to those techniques and procedures used to control the many operations performed on information to accomplish the agency's objectives, but do not extend to the essential managerial determination of the need for and uses of information in relation to any agency's mission. In this context, information management includes: data collection, validation and transformation; information processing or handling; record keeping; information control, display, and presentation; and finally standardization of information management operations.

Effective application of these processes contributes importantly to the Privacy Act objectives of maintaining accurate, timely and complete data. An examination of current practices should, therefore, be a first order of business to determine whether modifications or enhancements are needed. Changes to current practices will be implemented with differing degrees of additional expense and operational overhead depending upon the extent to which good management practices already exist.

The information management guidelines presented below are grouped into major categories to facilitate the explanation of their role. *Every practice presented may not be required at every data processing installation.* Selection of practices for implementation from those identified below should reflect their relevance to the specific agency environment. For instance, an installation which processes only personal data could elect not to label volumes of storage media containing personal data.

4.1. Handling of Personal Data

- Prepare a procedures handbook which describes the precautions to be used and obligations of computer facility personnel during the physical handling of all personal data. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act.
- Label all recording media which contain personal data. Labelling such media will reduce the probability of accidental abuse of such data, and also will aid in fixing the blame in the event of negligent or willfully malicious abuse.
- Store personal data in a manner that conditions users to respect its confidentiality; e.g., under lock and key when not being used.
- If a program generates reports containing personal data, have the program print clear warnings of the presence of such data on the reports.
- Color code all computer input/output card trays, tape reels, disk pack covers, etc., which contain personal data, so that they can be afforded the special protection required by law.
- Keep a record of all categories of personal data contained in computer-generated reports to facilitate compliance with the requirements that agencies identify all such data files and their routine use by the agency.
- Carefully control products of intermediate processing steps, e.g., scratch tapes and disk packs, to ensure that they do not contribute to unauthorized disclosure of personal data.
- Maintain an up-to-date hard copy authorization list of all individuals (computer personnel as well as system users) allowed to access personal data for use in access control and authorization validation. Operations and systems personnel should be considered privy to any data they handle since anomolous conditions may cause or require their knowledge of data contents.
- Maintain an up-to-date hard copy data dictionary listing the complete inventory of personal data files within the computer facility in order to account for all obligations and risks.

4.2. Maintenance of Records to Trace the Disposition of Personal Data

- Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility.
- Log each transfer of storage media containing personal data to or from the computer facility.
- Maintain logbooks for terminals that are used to access personal data by system users.

4.3. Data Processing Practices

- Use control numbers to account for personal data upon receipt and during input, storage and processing.
- Verify the accuracy of personal data acquisition and entry methods employed.
- Take both regular and unscheduled inventories of all tape and disk storage media to ensure accurate accounting for all personal data.
- Use carefully-devised back-up procedures for personal data. A copy of the data should be kept at a second location if its maintenance is required by law.
- Create a records retention timetable covering all personal data and stating minimally, the data type, the retention period, and the authority responsible for making the retention decision.
- After a computer failure, check all personal data which was being processed at the time of failure for inaccuracies resulting from the failure.

- If the data volumes permit economic processing, some sensitive applications may use a dedicated processing period.
- Files created from files known to contain personal data should be examined to ensure that they cannot be used to regenerate any personal data. A formal process must be established for the determination and certification that such files are releasable in any given instance.
- In aggregating data, give consideration to whether the consequent file has been increased in value to a theft-attracting level.
- When manipulating aggregations and combinations of personal data, make impossible the tracing of any information concerning an individual. Steps should be taken such that no inference, deduction, or derivation processes can be used to recover personal data.

4.4. Programming Practices

- Subject all programming development and modification to independent checking by a second programmer, bound by procedural requirements developed by a responsible supervisor.
- Inventory current programs which process or access personal data; verify their authorized usage.
- Enforce programming practices which make the use of personal data in any computer program clearly and fully identified.*
- Strictly control and require written authorization for all operating system changes that involve software security.

4.5. Assignment of Responsibilities

- Make a designated individual responsible for examining installation practices in storage, use and processing of personal data, including the use of physical security measures, information management practices and computer system access controls. He should consider both internal uses and the authorized external transfer of data, reporting any risks to the relevant management authority.
- Make a designated individual responsible during each processing period (shift) for insuring that the facility is adequately manned with competent personnel and that the policies for the protection of personal data are enforced.
- Ensure that all employees engaged in the handling or processing of personal data adhere to established codes of conduct.

4.6. Procedural Auditing

Whenever appropriate, conduct an independent examination of established procedures. Audits of both specific information flow and general practices are possible. The following points should be considered when developing an audit:

- Auditing groups can be established within organizations to provide assurance of compliance independent of those directly responsible.
- Independent outside auditors can be contacted to provide similar assurance at irregular intervals.
- Audit reports should be maintained for routine inspection and to provide additional data for tracing compromises of confidentiality.

5. Systems Security

Once physical security measures and information management practices have been established, managers of some large information systems will want to consider system-based methods for protecting data. These include user identification procedures, access auditing to trace activity in the system, and system mechanisms to control data access, all of which can be incorporated into today's systems. Some details of these methods and the situations to which they are applicable are described here.

5.1. Identification

The identification of each individual who is allowed to use a system is a necessary step in safeguarding the data contained in that system. Identification of users is in many instances actually a two-step process consisting of identification and authentication, i.e. a would-be user of a system states who he is and the system verifies that he is who he claims to be. Determination of identity can range from the personal recognition by a system employee of a user submitting a batch job to a fully automated system log-on procedure from a remote terminal. The chance for misidentification is much greater when jobs are submitted directly into an ADP facility from a remote site and this chance is increased when access to the facility is achieved over common carrier lines.

* See Section 6.5 of the "Guidelines for ADP Physical Security and Risk Management," referenced in the Appendix.

There are three categories of methods by which a person's identity may be established for the purpose of allowing access to an information system. The methods, which can be applied singly or in combination, are based on:

(1) Something the person *knows;*
(2) Something the person *has;*
(3) Something the person *is.*

The first category includes such things as passwords, the combinations to locks, or series of facts from an individual's personal background. The second category comprises such things as badges, cards with machine-readable information, and keys to locks. The third category consists of characteristics, such as a person's appearance, fingerprints, hand geometry, voice or signature. Identification based on "something a person is" includes recognition by guards, which is frequently the best defense against unauthorized access.

Badges, cards with machine readable information, or keys can be used for identification of users at terminals in remote locations, but some additional authentication procedure should also be considered. The physical security and procedural control of badges and keys, which frequently play a significant part in the identification process, are discussed in Section 3.1.

Passwords are perhaps today's most widely used identification technique for granting system access. They can be used to relate system users with specific system resources to which they are authorized access; they are also frequently associated with particular applications or information files. Because of their widespread use, considerable experience has been developed in the use of passwords. Considerations include:

- Passwords should be attributable to individuals in order to ascribe individual responsibility and reduce the likelihood of individuals giving out passwords to unauthorized coworkers. Passwords can be used not only to identify users, but also to control which data and other system resources they are authorized to use (see Section 5.2).
- Passwords should be easy to remember, but they should not be based on information such as a person's initials or birth date. It is best if the system administrators generate random passwords for users.
- Passwords should be changed at given intervals as well as whenever compromise is known or suspected.

5.2. System Access Controls

While identification can go a long way toward preventing unauthorized use of a system, it is still necessary to have limitations on the use of data. Access controls can serve that purpose. They are the means of preventing a user, once having gained access to the system, from reading, altering or destroying any data he wishes. Lists (or even classes) of users authorized to perform certain activity or to access specified data or combinations of the two can be developed and stored in the computer to insure that only authorized data activity occurs.

Implementation considerations are:

- Some commercially available systems already have data access controls built in. In many cases these controls are not being used because some additional effort is sometimes required in reprogramming current applications. However, if needed, such access controls could provide a significant increase in data protection.
- Applications programs can have their own access control mechanisms built in if the operating system does not provide them.

5.3. Access Auditing

Closely allied to the access control mechanism is the ability to account for *who* had access to *which* data. The control mechanisms form the basis for reports on data usage. These reports, known as audit trails, can be designed to list all system activity, all data accesses, unusual activity, etc. Such a report can be examined for unauthorized disclosures of data.

The same auditing capability which produces the above reports can be used to enhance the automated log of system use presently utilized for charge accounting. Some benefits of such use may partially offset the costs of implementing the access control mechanism. A security log and audit will result in the recovery of some costs due to the more accurate charging for system use, better determination of causes of system failures, and, when properly exploited, greater facility for data base recovery in case of failure.

5.4. Network Systems

Risks to computer data become more significant during transmission among computer systems in a network or between a computer data bank and remote terminals. The potential of intentional compromise increases with the amount of data accessible in a network, the number of possible users of that data, and the geographic distribution of the network. In particular, there is the possibility that data may be intercepted while it is being transmitted. Also, messages may be modified or others substituted,

and false identities may be claimed by unauthorized network users or terminals. Finally, addresses may be accidentally or intentionally changed, sending traffic to the wrong destinations.

Although a proposed Federal standard for encryption is presently being prepared, it is neither presently available nor necessarily justified for protecting transfers of personal data. For the convenience of designers of future systems; encryption is discussed in Section 5.5.2. However, other steps for protection of data in networks are possible. Suggested considerations are:

- Establish requirements for identification, access control and access auditing methods in networks as in any other systems.
- Establish controls on network access. A useful procedure is to draw a diagram of the computer network architecture specifying the locations of all components (computers, terminals, communication paths). Each component should be labeled with a unique identifier, and a list of the people and terminals authorized to use the network should be prepared. For each, the list should include: identifier, terminals authorized for use, data access privileges and access restrictions. Rules for modifying this list, adding and deleting individuals or access privileges, should be developed.
- Log transfers of personal data in a security audit trail to account for disclosures of data.
- Verify special requests involving sensitive data to the computer operating system even though initial system access has been granted to the requestor.
- Assign a network security officer.

5.5. Planning for Future ADP Systems

It is important for those involved in planning future systems to be aware of forthcoming technological developments in computer security in order that the new technology can be incorporated into the design of the systems from their inception. The following discussions are offered for this reason.

5.5.1. Internal Controls

Current computer technology does not provide provable solutions to certain internal system security problems. These security problems arise from the fact that indirect and sophisticated penetration can bypass any ad hoc security controls. While this kind of security problem exists, it is important not to overestimate its probability of occurrence. Such an attack will occur only when a skilled individual is motivated to dedicate an extensive effort to planning a deliberate penetration of an ADP system, and historically the motivation has been financial. The various system safeguards previously discussed will make it more difficult to plan and carry out an indirect attack. Security logs may be the most effective in deterring such attacks as they raise the probability of detecting the attack and of apprehending the attacker. It may not be cost-effective to provide additional safeguards specifically to counter sophisticated indirect attacks, such as penetration of an operating system.

Advancing technology may soon lead to very cost-effective protection against attempts to bypass internal system access controls. Those who will not be procuring computer systems until the late 70's or early 80's may be able to take advantage of such technology if the current research in this area is successful.

In the meantime, the following guidance is provided for current and future data processing installations which are dependent on current computer technology.

- Segment the data processing activity in such a way that the sensitive information is not totally available, nor vulnerable, at any one time or place.
- Personal data which may be subjected to intensive computer security threats should be processed with stringent physical and information management controls which provide the needed security; for example, the data could be processed in a dedicated mode or remote programming access to the system could be restricted during the processing of this information.

5.5.2. Data Encryption

The planning and design of a data processing network should provide safeguards so that no one can utilize the communication facilities to obtain sensitive information being transmitted through the network. Under certain circumstances of high risk, data encryption may be needed for the protection of personal data in computer networks. The following material is presented as background information for the planners of future networks.

Encryption is achieved either through a secret process or through a commonly known process which depends on a secret parameter. In order to allow compatibility of encryption processes within the typical variety of network compo-

nents, the latter method is preferred. The encryption process is generally specified in an algorithm (a set of rules or steps for performing a task) and the secret parameter supplied to the algorithm is called the key. Decryption is the inverse process.

The National Bureau of Standards published an encryption algorithm in the *Federal Register* of March 17, 1975, which satisfies the primary technical requirements of a data encryption standard. It is planned that this standard will be promulgated as a Federal Information Processing Standard (FIPS). The algorithm may be implemented in presently available electronic technology.

Control devices must be constructed to format the data for the encryption device and to transmit and receive the encrypted data. These will depend on the computer component and the communication network to which it is attached.

Identification, access control and access auditing should be implemented within a computer system before sophisticated encryption devices are procured for the protection of data in networks. However, assuming a defined need for encryption and the availability of encryption devices and any necessary network control devices, the following should be considered:

- Using the network diagram and the authorization list described in Section 5.4, the diagram should be augmented by locating encryption devices so as to protect personal data at places where data is vulnerable to network security threats.
- Data encryption keys must be created and distributed to authorized network personnel. They must be protected at all times and changed frequently. Periodic changes are suggested and immediate changes are necessary if a compromise has occurred or is thought to have occurred.

Appendix

Computer Security and Privacy Publications of the Institute for Computer Sciences and Technology

National Bureau of Standards

Title	Abstract	Source	Catalog No.	Cost
Controlled Accessibility Bibliography (NBS Technical Note 780; June, 1973)	A bibliography of works dealing with the hardware and software technological measures available in a computer system for the protection of data.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.46:780	$ .55
Controlled Accessibility Workshop Report (NBS Technical Note 827; May, 1974)	A report of the NBS/ACM Workshop on Controlled Accessibility, December 1972, Rancho Santa Fe, California. The workshop was divided into five separate working groups: access controls, audit, EDP management controls, identification, and measurements. The report contains the introductory remarks outlining the purpose and goals of the workshop, summaries of the discussions that took place in the working groups and the conclusions that were reached.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.46:827	$1.25
Executive Guide to Computer Security (NBS Special Publication; May, 1974)	This booklet was prepared for non-ADP executives and managers. It is intended to introduce management to the necessity for computer security and the problems encountered in providing for it.	Systems and Software Division Room A247, Technology Building National Bureau of Standards Washington, D.C. 20234	None	No Charge
Guidelines for Physical Security and Risk Management (Federal Information Processing Standards Publication 31; June, 1974)	This publication provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. It treats risk analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness and security audit. Statistics and information relevant to physical security of computer data and facilities are presented. There are also many references to other, applicable publications containing more exhaustive treatments of specific subjects.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.52:31	$1.35

U.S. GOVERNMENT PRINTING OFFICE : 1975—O-578-379