

BY THE COMPTROLLER GENERAL

Report To The Congress

OF THE UNITED STATES

8920

Automated Systems Security-- Federal Agencies Should Strengthen Safeguards Over Personal And Other Sensitive Data

At a time when increasing reliance is placed on computers and rapidly advancing ADP technology, security procedures for systems processing personal and other sensitive data generally were inadequate. Agencies

- lacked comprehensive computer security programs addressing technical, administrative, and physical safeguards;
- did not place the computer security functions at a sufficiently high level, with independence from operating functions, to preclude preemption by operational priorities;
- did not understand and employ risk management techniques for economic selection of safeguards;
- through lack of appreciation did not take advantage of the technical guidance provided by the National Bureau of Standards; and
- did not effectively use their internal audit resources.

f/c

The Office of Management and Budget has agreed that correcting these matters is the responsibility of agency and department heads.



168420
003299

Report

LCD-78-123
JANUARY 23, 1979



COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-115369
B-130441
B-173761

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

This report addresses the status and effectiveness of automated systems security programs in the Federal Government and is in response to a request by the Chairman of the Subcommittee on Government Information and Individual Rights, House Committee on Government Operations.

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).

Copies of this report are being sent to the Director, Office of Management and Budget; to the heads of departments and agencies involved in our review; and to the heads of other major recordkeeping executive departments and agencies.

James B. Stites
Comptroller General
of the United States

COMPTROLLER GENERAL'S
REPORT TO THE CONGRESS

AUTOMATED SYSTEMS SECURITY--
FEDERAL AGENCIES SHOULD
STRENGTHEN SAFEGUARDS OVER
PERSONAL AND OTHER SENSITIVE
DATA

D I G E S T

Federal agencies GAO surveyed did not have a centrally directed program to protect effectively personal and other sensitive data in computer systems. Programs fell short of being comprehensive and top management support was lacking. This was, in part, because upper management either did not recognize or adequately appreciate their responsibilities in this area or recognize the potential for invading the privacy of people or organizations served by the agency and for damage to agency program operations.

GAO surveyed selected agencies in 1977 because of the generally high level of congressional interest in Federal information policies following the enactment of the Privacy Act and the Freedom of Information Act Amendments in 1974. Subsequently, GAO was specifically requested to examine and report on the status and effectiveness of major Federal agencies' computer security programs by the Chairman of the House Subcommittee on Government Information and Individual Rights, House Committee on Government Operations.
(See p. 1.)

GAO's review included 10 civil agencies but excluded the highly specialized area of controls over national security classified data in Defense agencies. (See p. 2.) Many other agencies throughout the Government are experiencing to varying degrees some of the same weaknesses. In fact, GAO's review further confirmed automated system security and control problems disclosed in many prior GAO published reports. (See p. 3.)

In a larger sense, these findings have potential applicability wherever computers are used intensively. This is because of the pervasiveness of the underlying causes of poor data security. Modern computer based information systems represent relatively recent technology that has introduced many new threats adding to management problems of maintaining data at acceptable levels of integrity and security. (See pp. 7 and 8.)

WEAKNESSES IN AGENCY PROGRAMS FOR COMPUTER SECURITY

GAO focused on weaknesses in the agencies' systems of management controls, including appropriate organizations, monitoring and reporting, use of risk analysis, and use of independent internal audits. (See pp. 10 27, and 47.)

Particular attention was given to the degree of agencies' efforts to organize and implement broadly conceived programs of data security in compliance with the Office of Management and Budget (OMB) directives and related computer security guidance published by the National Bureau of Standards, Department of Commerce. (See p. 10.)

Although all agencies reviewed had some elements of a computer security program in varying stages of being, they lacked the management support needed to be truly comprehensive. (See p. 10.)

Security programs usually were not developed from the perspective of the total data system; consequently, any weak link could result in ineffective security. For example, the scope of most security programs did not cover data in all media and in all stages of the data life cycle nor did they consider all possible threats at all locations involved with the agencies' data. Additionally, many programs did not have written plans, policies, and procedures. (See p. 11.)

X Also, management generally did not place the computer security function at a sufficiently high level, with independence from operating functions, to preclude preemption by operational priorities. Thus, authority to recommend and enforce security measures was seriously lacking. Agencies did not establish clear responsibilities of individuals and organizations. (See p. 14.)

X Management generally was giving inadequate attention to monitoring the aspects of computer security in their organizations to be sufficiently informed on how their security measures were working. Management was not receiving the feedback necessary for control of computer data security. (See p. 20.)

X Agencies usually had selected computer systems safeguards intuitively rather than on a cost-effectiveness determination which would take into account the degree of sensitivity and vulnerability of the information to be protected. This risk management concept, which should be applied in all determinations to select economically feasible safeguards considering the particular environment where the data is processed, was generally not employed. (See p. 27.)

X Security programs should but usually did not address all of the necessary elements of technical, administrative, and physical safeguards. In many cases, attention had been given by technicians and lower and middle level managers to the obvious and traditional safeguards. However, safeguard protection that required upper level management and administration were neglected. (See p. 30.)

INTERNAL AUDIT

At a time of increasing reliance on computers and rapidly advancing automated data processing technology, internal audit can be a

vital resource for keeping management informed on data security requirements and how well these responsibilities are being met. However, at the agencies surveyed, independent internal audit generally was not significantly involved in assessing computer based systems controls or conducting more conventional security compliance audits.

Agency internal audit was not significantly involved in computer security because of a lack of technical expertise. Discussions with Internal Audit officials revealed that the expertise needed to challenge security shortcomings has not been developed because top management has not tasked internal audit in a computer security role. (See p. 47.)

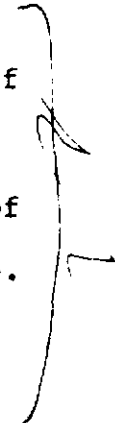
OMB's GUIDANCE TO AGENCIES

Although OMB has stressed that data security and integrity are the responsibilities of the heads of departments and agencies, GAO found that agencies did not take the initiative to meet these responsibilities.

OMB's policy guidance and technical guidance provided by the National Bureau of Standards was largely ignored and not used to advantage. Consequently, the agency security programs did not reflect the intent of this guidance.

CONCLUSIONS

OMB issued Circular A-71, TM-1--on Security of Federal Automated Information Systems--after completion of this review. The circular requires action by agency top managers which could contribute greatly to correcting many of the computer data security problems addressed in the GAO report. The circular is directive. It is also quite comprehensive. It requires agency heads to report on their plans to to comply. (See p. 23.)



Specifically, the circular promulgates policies and responsibilities for the development and implementation of computer security programs by all executive departments and agencies: It further addresses the general requirement for agencies to implement a computer security program; it establishes specific requirements for the development of management controls to safeguard personal, proprietary and other sensitive data in automated systems; and it defines a minimum set of technical controls to be incorporated into each agency computer security program. (See app. IV.) Therefore, it sets an appropriate framework for agencies' initiatives to correct their data security problems.

RECOMMENDATION TO OMB

GAO views a leadership role by OMB as vital to maintaining the momentum that Circular A-71 should impart to computer security in Federal agencies. GAO is concerned that agencies may lose sight of the stated purpose of the directive, i.e., that agencies develop and implement computer security programs with a scope to protect personal, proprietary and other sensitive data. The circular further addresses certain specific technical requirements. Accordingly, GAO sees a critical need for OMB to follow up on the circular's requirement that agencies prepare and submit plans for compliance. (See p. 23.)

The Director of OMB should arrange for independent reviews by persons knowledgeable in computer security of the plans of departments and agencies responding to Circular A-71. OMB should critique agencies on the adequacy of their plans for computer security using the findings and recommendations to heads of agencies contained in this report as well as the requirements set forth in Circular A-71. (See p. 23.)

RECOMMENDATIONS TO HEADS
OF FEDERAL AGENCIES

✓ All agencies should strengthen their computer data security and integrity, highlighted as follows.

--Computer security programs should be comprehensive.) They should include plans, policies, and procedures in writing that clearly establish responsibilities throughout the organization. (See p. 25.)

for AG
--Agencies should establish a computer security administration function with independence from computer operations.) This organization should report directly to or through a principal official who reports directly to the agency head. (See p. 24.)

--Programs should provide for feedback for management control, both in routine monitoring and reporting and in independent internal audits. (See pp. 25 and 52.)

--Risk management should be provided for and should be on the perspective of the total data systems. (See p. 46.)

└ --Security planning should anticipate training needs, particularly for risk management. (See pp. 25, 46, and 52.)

OMB's COMMENTS

OMB representatives indicated that GAO's examination of the status and effectiveness of computer system security programs provided information and recommendations which would be used and followed up in their own assessments of Federal agencies' plans to comply with their Circular A-71 and other requirements.

OMB is placing a high priority on efforts over the coming year to improving security programs in agencies and has organized a task force to accomplish reviews of agencies' plans. This effort is coupled with OMB's broader concerns for improving controls in agencies over fraud and abuse. OMB indicated that attention by agencies' inspector general functions will be focused on correcting these matters in recognition that they are important responsibilities of agency and department heads.

OMB expressed some concern that GAO's recommendation for organizing a highly placed computer security administration as a staff function, independent from computer operations, might cause difficulty with the agency head's span of control. That is, too many functions are now competing for top-level attention and this would add one more. GAO intends its recommendation to be sufficiently broad to allow each agency maximum flexibility in its implementation in a wide variety of agency organizations.

GAO agrees with OMB that elements of this security function such as monitoring, inspection, and audit could be placed under the inspector general function. But GAO sees the need for identification of a focal point at a high level, independent from responsibility for computer operations, to develop and oversee an automated systems security program. The security program itself should be promulgated by a directive and guidance issued by the agency head. (See p. 24.)

C o n t e n t s

		<u>Page</u>
DIGEST		i
CHAPTER		
1	INTRODUCTION	1
	Congressional interest	1
	Findings from our prior studies	3
	Federal information policies	6
	Operational considerations	8
	Scope of review	8
2	COMPUTER SECURITY ORGANIZATION, PLANS, AND PROCEDURES	10
	Comprehensive computer data security programs	10
	A master program plan	11
	Implementation responsibilities	13
	Conclusions	13
	Computer data security organization	14
	Placement of the security administration function	14
	Defining responsibility for security administration	16
	Conclusions	19
	Security monitoring and reporting	20
	Procedures and implementation	20
	Security monitoring by operating personnel	22
	Conclusions	22
	Conclusions	23
	Recommendation to OMB	23
	Recommendations to heads of depart- ments and agencies	24
	OMB's comments	25
3	SELECTING AND IMPLEMENTING SAFEGUARDS	27
	Risk analysis and safeguard selection	27
	Safeguards	30
	Administrative considerations	31
	Technical safeguards incorporated into systems	40
	Physical safeguards for data and facilities	41

	<u>Page</u>
CHAPTER	
The HEW task force review	44
Conclusions	44
Recommendations to heads of departments and agencies	46
4 INTERNAL AUDIT INVOLVEMENT	47
The evolving role of internal audit	48
Internal audit capabilities	50
Departmental ad hoc task force	51
Conclusions	51
Recommendations to heads of departments and agencies	52
APPENDIX	
I Need for and benefits of comprehensive security planning	53
OMB's directives implementing the Privacy Act	53
OMB's supplemental directive on risk assessment	55
OMB's new directive establishing computer security policies and control procedures	55
Stanford Research Institute study	57
A government/industry conference	58
II Reference sources	61
List of GAO reports	61
Multiagency or Government-wide reports addressing selected computer security or control issues	61
Reports assessing security programs or the controls in selected agency computer systems	61
Selected central agency guidance	62
List of other references	63
III List of agencies and locations covered in survey	65

APPENDIX

IV	OMB Circular No. A-71, Transmittal Memo No. 1, Issued July 27, 1978	68
----	--	----

ABBREVIATIONS

ADP	Automated data processing	
FIPS	Federal Information Processing Standards	
GAO	General Accounting Office	
HEW	Department of Health, Education, and Welfare	— 22
IRS	Internal Revenue Service	— 4
NAC	National Agency Check	
NBS	National Bureau of Standards	— 126
OMB	Office of Management and Budget	— 27

CHAPTER 1

INTRODUCTION

This report presents an assessment of the safeguards and controls for protecting personal and other sensitive data processed in computer systems of selected Federal agencies. The review responds to both specific and general expressions of congressional interest in issues involving the confidentiality and security of information.

CONGRESSIONAL INTEREST

We initiated a survey of selected agencies in April 1977 because of the generally high level of congressional interest following the enactment of the Privacy Act and Freedom of Information Act Amendments in 1974. Subsequently, by letter of November 11, 1977, we were specifically requested to examine and report on the status and effectiveness of major Federal agencies' computer security programs by the Chairman of the House Subcommittee which has oversight responsibilities for these acts (Government Information and Individual Rights Subcommittee, House Committee on Government Operations).

The Subcommittee's concerns were raised by the Department of Health, Education, and Welfare's (HEW's) departmental ad hoc task force report that found automated data processing (ADP) systems security was not meeting the department's published minimum acceptable standards. (See pp. 13, 44, and 51.) The constituent agencies throughout that department, among numerous other deficiencies, lacked organized security programs, experienced weak management controls over system development, and provided inadequate direction in risk management. The Subcommittee Chairman also expressed an interest in the outcome of our separate review of computer system security at the Social Security Administration, subsequently published on June 5, 1978.

In making his request to us, the Subcommittee Chairman wanted to know if the conditions at HEW were widely prevalent in Federal agencies. The Subcommittee was briefed in November 1977 and April 1978 and we advised it that our survey showed many departments and agencies, like HEW and the Social Security Administration, have not acted to meet this challenge by developing comprehensive security programs.

Although the approaches to providing safeguards varied among agencies, they all showed serious weaknesses attributable to (1) absence of top-level security planning and procedures to carry out comprehensive programs, (2) lack of independent security organizations with authority to recommend and enforce security measures, and (3) inadequate provisions for continuous monitoring and reporting weaknesses in security safeguards. Moreover, the pervasiveness we found tends to confirm weaknesses reported in our numerous prior reviews.

The Subcommittee agreed that a report analyzing the results of our self-initiated, ongoing survey in selected agencies would address the Subcommittee's concerns and because of general congressional interest could be addressed to the Congress as a whole.

Although the conditions disclosed in the HEW task force report were very serious, we believe HEW should be commended for its recent efforts to cope with these problems. The Chairman of the Subcommittee on Government Information and Individual Rights stated: 1/

"With respect to HEW's efforts, I would be remiss if I did not give the Department credit for the initiative it has shown in both establishing security standards and undertaking a self-assessment of compliance with those standards. Moreover, I think it is important to note that Secretary Califano has approved the task force recommendation for a vigorous corrective action program. If the proposed schedule is adhered to, the existing deficiencies will be remedied within the current fiscal year."

We believe actual improvement is dependent upon how effectively procedures are implemented and that this will require a strong and continuing showing of management support in HEW.

In this review we initially examined only civil agencies, and excluded protection of national security data or

1/The Subcommittee Chairman's comments on the task force report were printed in the Congressional Record dated Nov. 11, 1977, page H. 12314.

computer security programs in general, of the Department of Defense and its component services and agencies. Defense activities were not included because of the extensive internal audit efforts which were ongoing at the time of our review. A separate assessment is being made of these audit efforts and findings. Our work here is focusing on the broader implications for security program weaknesses. The indications at this point are manifold that Defense agencies have experienced difficulties in each of the broad areas discussed in the following chapters of our present report. These areas include clarification of policies and regulations to define the scope of security programs and responsibilities, independence of the security function, applying risk management techniques, compliance with security requirements, and internal audit resources and coverage.

While we have not completed our work in Defense agencies, we would like to commend the initiatives taken in that Department to evaluate security practices. At the Department of Defense, we have identified and are analyzing more than 70 audits of computer security currently in process or recently completed. There has been interest at all levels of Defense as manifest by the broad-ranging efforts to conduct self-assessments of compliance with security requirements. HEW and Defense are the two agencies coming to our attention that undertook the task of self-assessment on the most comprehensive basis.

FINDINGS FROM OUR PRIOR STUDIES

Our present report focuses on a study of the management controls needed to achieve effective programs of computer systems security in Federal agencies. We have referenced several other published GAO reports which involved reviews addressing a major agency system or examining other broad concerns for computer systems controls and safeguards. (See listing in app. II.) Closely related to our current report is our recent report 1/ on security techniques for protecting personal information in an expanding Federal computer network environment which addressed concerns of the Congress over concepts of a national data center or major Federal computer networks.

1/"Challenges of Protecting Personal Information In An Expanding Federal Computer Network Environment"
(LCD-76-102, Apr. 28, 1978).

In that report we observed that managers are generally aware of the notion that the state-of-the-art in computer security is such that total security is not practicable to achieve and still maintain functional effectiveness. The report relates that when cost is considered total security would not be practicable in any environment--human or computer--and that decisions on security must make the cost of subverting a system greater than the monetary benefits or the cost in punitive terms, i.e., using risk management concepts. The cost of recreating records which could be destroyed is another factor.

While we have not undertaken in this assignment to chronicle examples showing cost and other adverse effects that have resulted from lax controls in computerized information systems, this was the subject of one of our previous reports. 1/ In that report we observed that computer systems have added a new dimension for potential crime. Information on computer-related crimes in Government is difficult to gather because they are not classified as such by investigative agencies. But we learned of 69 instances of improper use of computers in Federal programs resulting in losses of over \$2 million. We concluded:

"Most of the cases GAO examined did not involve sophisticated attempts to use computer technology for fraudulent purposes rather, they were uncomplicated acts which were made easier because management controls over the systems involved were inadequate."

* * * * *

"Management needs to pay more attention to the importance of these controls."

Another report 2/ showed that computers in Federal departments and agencies annually issue unreviewed payments

1/"Computer Related Crimes in Federal Programs"
(FGMSD-76-27, Apr. 27, 1976).

2/"Improvements Needed In Managing Automated Decision-making by Computers Throughout the Federal Government"
(FGMSD-76-5, Apr. 23, 1976).

(excluding payrolls) involving \$26 billion and affect transfers of additional billions of dollars in Government assets. The actions are often wrong. They cost the Government large sums of money; exactly how much no one knows. Controls in automated systems involved in the administration of monetary assets are clearly needed to reduce the potential for intentionally caused losses to the Government and illegal personal gain to individuals.

That major Federal agency programs can be jeopardized by computer system security vulnerabilities has been repeatedly demonstrated in our prior reports. For example, in our recent report 1/ furnished to the Subcommittee on Government Information and Individual Rights (see p. 1), we observed,

"Social Security maintains millions of records on workers and beneficiaries in automated data banks and files. These records constitute a valuable national resource that must be safeguarded against alteration, destruction, abuse, or misuse. They contain valuable private personal information necessary to support present and future Social Security benefits.

"Social Security did not have an ongoing centrally directed program to protect its records. GAO recommends that the security weaknesses identified in this report be corrected and that Social Security continue to pursue an active and aggressive security program to assure the Congress, the public, and the beneficiaries that this valuable national resource is properly safeguarded."

Because computer systems are an integral part of agency management systems for administering most programs, in most cases it is readily apparent that safeguards are needed to assure continuity of operations. This is becoming an increasing concern to users of computer systems in private industry as well as in Government.

1/"Procedures to Safeguard Social Security Beneficiary Records Can and Should be Improved" (HRD-78-116, June 5, 1978).

When Federal agencies propose new systems without adequate attention to safeguarding sensitive data, their proposals are in jeopardy. For example, in 1970, the secretary of a department approved the proposal that an overall ADP plan be developed to achieve effective use of ADP resources. In 1974 when a request for proposals for new equipment was released, detailed plans had not been developed. GAO recommended that user requirements be determined and that security requirements to adequately protect personal or sensitive data be comprehensively planned before proceeding with the procurement. 1/ The system proposal was subsequently cancelled.

More recently other proposed system upgrades have, because of concerns for data security, experienced difficulty obtaining funding through appropriations 2/ and proposed procurements have experienced difficulties and bid protests were encouraged because of security issues.

FEDERAL INFORMATION POLICIES

Computer systems security is essentially the same regardless of what is being protected; the relevant question is how much security is needed to protect specific data. Interest in data security as an issue has been elevated in recent years because of concerns over privacy by the Congress and the public.

The concerns for protecting sensitive data from alteration, destruction, or misuse were recognized in Federal information policies enacted or amended by the Congress in 1974 and now being implemented under OMB's direction. (See app. I.) Under the Privacy Act of 1974 (5 U.S.C. 552a) this means a variety of measures protecting the personal privacy of individuals whose records are compiled in Federal agency systems. It includes requirements for safeguards to protect the confidentiality of information and controls to assure data integrity.

1/See our report entitled "Improved Planning--A Must Before a Department-Wide Automatic Data Processing System is Acquired for the Department of Agriculture" (LCD-75-108, June 3, 1975).

2/"Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, Jan. 17, 1977).

Under the Freedom of Information Act amendments of 1974 (5 U.S.C. 552) the Government's policy of generally favoring openness of records recognizes--under the legislation's enumerated permissive exemptions--that broad categories of information may need to be protected from disclosure because of the data's sensitive nature. This is to protect certain cited interests, in addition to personal privacy, such as national security; internal memoranda, rules, and practices of an agency; business data--trade secrets and commercial or financial information; and investigatory records compiled for law enforcement.

The Congress intended the two acts to work together generally to assure citizens their rights of access to Government records and rights of personal privacy, balanced against the Government's need to maintain confidentiality. The legislation was designed to prevent harmful effects of improperly releasing such data or possible inadvertent disclosure of information.

The legislation provided much latitude to individual agencies as to how these goals should be implemented by agency records managers. This is to say that there is a technical gap between accomplishment of the definitive requirements of the acts and the application of manual and computer information management science by the Government records keepers. The lack of uniform criteria has resulted in significant differences in the policies and procedures promulgated--or the degree they are addressed--by the various agencies, and a general confusion exists among the agencies as to what constitutes adequate protection of personal and other sensitive information.

These conditions were recognized by two commissions chartered by the Congress to examine and report on such information issues. The Privacy Protection Study Commission in appendix 5 to their report states at pages 49 and 50:

"Setting forth broad public-policy objectives while allowing for various implementation alternatives and strategies does, however, create a need for reasonable definitive guidance to operating personnel on what constitutes acceptable levels of performance in certain areas."

* * * * *

"The problem yet to be addressed in any broad and effective way, at either the State or Federal level, is how to translate the broad social goals of privacy and fair information practice legislation into precise steps which computer scientists and managers of automated systems may follow in order to achieve acceptable levels of performance."

The Commission on Federal Paperwork expressed concerns about the lack of a central Federal policy on inter-agency information sharing to reduce the burden on the public in providing information. The Commission pointed out that this results from a myriad of laws which regulate the collection, use, and dissemination of data. They pointed to the Privacy Act of 1974, the Freedom of Information Act, the Federal Reports Act, and some 200 other statutes regulating the use of specific, so-called "confidential" information.

Confronted with these circumstances it is understandable that agencies have been generally confused about what constitutes an appropriate security program and the level of security needed to protect various specific data. The reports of the two Commissions are listed in appendix II.

OPERATIONAL CONSIDERATIONS

The Federal Government is the largest user of computers in the world. As of January 1978, the Federal Government was using 11,328 computers. We estimated the costs of operations to be over \$10 billion annually.

Many agencies' operations would be on a considerably narrower perspective without computers. The National Aeronautics and Space Administration could not carry out its space programs without them. The accomplishments of the Internal Revenue Service processing about 125 million income tax returns annually and the Social Security Administration's annual payments of over \$84 billion could not be efficient without computers.

The environment in which government places a particularly heavy reliance on modern computer capability holds potential for fraud, misuse of data, and economic loss, or loss of agencies' continuity of operations.

SCOPE OF REVIEW

We interviewed agency officials and reviewed records and documents describing computer security plans, policies,

procedures, and organizational responsibilities. On a selected basis, we also examined compliance with, and the effectiveness of, technical, administrative, and physical safeguards which were, or could be, employed by these agencies. In many cases, examples we reported were identified by agencies as a result of monitoring or audit efforts.

In this report, we are not identifying details of specific security weaknesses with the particular agencies and locations because of a mutual concern that these system vulnerabilities should not be further exposed.

We assessed agencies' compliance with OMB's directives and related computer systems security guidance published by the National Bureau of Standards (NBS), Department of Commerce. Our analysis shows the conditions prevailing at the time of the field work of our survey, generally in the latter half of 1977 and first half of 1978.

The 10 civil agencies and location of activities covered in our survey are identified in appendix III.

CHAPTER 2
COMPUTER SECURITY ORGANIZATION,
PLANS, AND PROCEDURES

The agencies we surveyed did not have ongoing, centrally directed computer security programs to provide adequate protection for the integrity and confidentiality of personal and other sensitive information. Although the approaches to providing safeguards varied among agencies, they all showed serious weaknesses attributable to (1) absence of top-level security planning and procedures to carry out comprehensive programs, (2) lack of independent security organizations with authority to recommend and enforce security measures, and (3) inadequate provisions for continuous monitoring and reporting weaknesses in security safeguards. The agencies lacked top management involvement and support needed to achieve these measures to a degree necessary to accomplish more than a minimally effective security program.

To be comprehensive, data protection must be considered from a total system perspective; that is, the protection of data must be considered from its origination to its final destruction. Furthermore, protection of data in any form or process must be multifaceted; the capability of an information processing system to protect sensitive data is contingent upon the use of technical, administrative, and physical safeguards as appropriate.

The agencies we surveyed did not capitalize on guidance for attaining standards published by OMB in directives on computer and data security and by NBS in technical guidance. We found this guidance neglected because agencies lacked concern or did not appreciate the intent. (See app. I for our discussion of OMB directives and app. II for a list of NBS guidance.)

COMPREHENSIVE COMPUTER DATA
SECURITY PROGRAMS

We did not find, in the agencies surveyed, what could be considered a comprehensive data or computer security program supported by complete operating instructions.

The directives and guidelines referenced in appendixes I and II of this report require agencies to establish appropriate security policies, plans, and procedures and assign

responsibility for developing, implementing, and maintaining comprehensive computer security programs. 1/

Our survey focused on evaluating the degree to which computer data security programs were comprehensive and the extent to which they were written in published policies and procedures disseminated to pertinent organizations within an agency.

A master program plan

A master plan is an indispensable requisite to an effective computer data security program because data security is multifaceted, involving many separate organizational components representing both computer system operators and users. Agencies we surveyed had not developed and published a written master plan, outlining policies, responsibilities, and procedures, and consequently have not established criteria needed for implementation and enforcement.

For example, one agency had implemented a manual for computer data security, which evidenced some degree of comprehensiveness. However, we found many deficiencies. It did not address risk analysis; there was no contingency plan for backup and recovery; the role of internal audit was not defined; and there were a number of other shortcomings. Another agency's manual had no coverage of technical security safeguards; it did not address administrative safeguards at other than computer sites (e.g., system design activities were not covered), or physical security at other than ADP

1/This is presently called for by OMB Circular No. A-71, Transmittal Memorandum No. 1, issued July 27, 1978, Subject: Security of Federal Automated Information Systems. The requirement was previously addressed in OMB's guidelines for implementing the Privacy Act of 1974: Circular A-108 issued in July 1975. There are two principal standards issued by NBS: Federal Information Standards Publication 31, issued in July 1974, Subject: Guidelines for Automatic Data Processing Physical Security and Risk Management and Federal Information Standards Publication 41, issued in May 1975, Subject: Computer Security Guidelines for Implementing the Privacy Act of 1974.

facilities (e.g., no coverage of remote terminals located at headquarters and in regions). One agency had a manual in effect which was oriented toward operating procedures and addressed computer data security only incidentally and superficially. Another agency had a computer data security manual/plan which pertained only to classified data; it had not published policies or procedures to encompass personal or other sensitive data systems. Two agencies within the same department had manuals approved but not yet implemented. One agency had no published overall plan or policies, but one division within the agency had its own security manual. The remaining three agencies we examined had no manual addressing security policies and procedures.

One of the agencies that did not have comprehensive written security plans, policies, or procedures, however, undertook a preliminary self-study recommending that a users' group be formed to plan for development of an agency-wide computer data security system. Before completion of our review at that agency, the users' group was organized, met, and recognized that an initial goal would be to establish written policy guidance for data security.

We found many examples of computer security provisions in agencies; however, they were fragmented and usually did not extend to protect all sensitive data or were not disseminated to all applicable elements within the organization. Classified data at one agency was processed at a secure center dedicated essentially to classified data, where protection expertise and procedures existed. The agency did not have policies or procedures for protecting unclassified sensitive data and there were no plans to develop protection for unclassified sensitive data processed at other locations.

Within another agency, at a facility we visited, the contractor/operator disclaimed to users any liability or responsibility for disclosures of sensitive data. A contractor official stated that emphasis is placed on protection of computer hardware and facilities; however, the contractor does not provide controls for data protection.

In yet another agency, the headquarters element responsible for computer data security did not issue written security procedures for its two data processing centers or its regions that process sensitive personal data over remote terminals.

Clearly, data or computer systems security in these agencies was not effective because of these shortcomings.

Implementation responsibilities

Clear definitions of responsibility and authority, once their proper places are determined, are necessary ingredients of a comprehensive computer data security program; without it, implementation is ineffective.

Three agencies we reviewed had defined responsibility for computer security procedures and measures to only a limited degree. One agency had not defined such responsibilities to any degree whatsoever.

As to responsibility for users, two agencies had defined this, but to only a limited degree. Three agencies had no written responsibilities of users of computer systems which processed personal or other sensitive data.

An example of how implementation of a security program fails when the responsibility chain is broken is one we observed in HEW. HEW's task force review (see p. 1) previously had discovered serious incidences of noncompliance in its agencies. At an agency's regional office we visited, personnel were unsure of their responsibilities for security. They did not have an appreciation for the applicability of NBS and the departmental standards to their operation because the agency level had not issued implementing instructions. This breakdown in the delegation of responsibility caused the departmental and NBS standards to be ignored.

Conclusions

We did not find a computer data security program that could be considered comprehensive and that was outlined in a set of published procedures. Furthermore, many agencies had not established clear responsibilities for implementing elements of programs which did exist.

Because of the heavy reliance of agencies on the integrity of computer systems and on the data, and due to the increasing potential for fraud, abuse, and operational setback and economic loss, development of comprehensive security programs should not be further postponed.

Heads of departments and agencies should assign responsibility at a high level of agency management to develop comprehensive computer data security programs without further delay. These programs should be developed from a total systems perspective, i.e., they should incorporate protection of data pertaining to the myriad of agency operations involved, from data origination to destruction. Programs should include plans, policies, and procedures, clearly set forth in writing. Implementation responsibility should be clearly delineated for all concerned, including systems designers, processors, users, and auditors at every level involved within the organization.

COMPUTER DATA SECURITY ORGANIZATION

Agencies have not made a conscious effort to structure their organizations in a way that will foster and promote data or computer security programs. Organizations involved in security administration generally were not independent of the data processing function, did not have direct contact with top management, and had little authority to recommend and enforce security measures. Responsibilities were not clearly defined or they were fragmented and overlapping. These conditions were responsible for weak computer security programs in Federal agencies that were surveyed.

Placement of the security administration function

We found the prevalent condition to be that the security administration function agencies had developed was embedded in ADP operations. The result is that security is sometimes overridden by operational commitments.

We recognized, in a prior report, ^{1/} the merits of an independent computer security function having overall responsibility for developing policy and monitoring the effectiveness of a computer data security program. In agencies maintaining substantial volumes of sensitive data, an organization should be established at the headquarters level to fulfill the security responsibilities of an agency head

^{1/}"Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, Jan. 17, 1977).

regarding the technical, administrative, and physical security of data processing. The organizational unit should be independent of the organizational elements responsible for the development and operation of computer systems and facilities. It should have authority sufficient to assure appropriate security. A similar organizational unit or responsible management official should be established at the data processing facility. The unit or official should be independent of day-to-day line operations and should have direct communication with the headquarters security activity.

We did find some acceptance of the principle of organizational independence in our present survey. In two agencies, the systems security officers were to some degree independent of the ADP operating function.

In one of these agencies, the responsibilities of the assistant administrator for national security included computer data systems security. He reported directly to the administrator of the agency. This security function was independent of ADP operations, which was the responsibility of another assistant administrator--for administration. While this independence was commendable, the responsibilities for data systems security did not go far enough; considerations of national security data took precedence over personal and other sensitive data considerations. Additionally, the security organization had responsibility for computer data security only at the headquarters, and none for regional office ADP functions.

In another agency, the systems security officer's immediate superior reported, in turn, to the second level of management in the agency--an associate commissioner for program operations. The ADP division and several program divisions were directly subordinate to the same second-level manager.

The other 8 agencies out of the 10 we reviewed had the security function placed with less independence from ADP operations and did not report to a top-level management official.

We observed instances in which these organizational structures caused computer data security to be in competition with agencies' day-to-day operational priorities. For

example, the system security administrator in one agency was responsible to the organization that performed ADP operations. On several occasions, he recognized and communicated a need for a backup plan to operate in the event of computer failure. However, his supervisors decided to postpone corrective action because of considerations they believed were more pressing priorities. Although this systems security administrator did have frequent communication with the head of the ADP division, to get his proposals implemented he had to get approval through three levels in the hierarchy between himself and the head of the ADP division. Following a reorganization which occurred during our review, this individual then had to go through a lesser number of levels but was still located in the organization that performed ADP operations.

In another agency where the ADP organization was responsible for technical security safeguards, the data base administrator recognized a need to generate an audit trail for monitoring the threat of an unauthorized access or input of sensitive data. However, ADP management established a higher priority, channeling resources to application software development rather than to technical security safeguards of this type.

In the operation of a new system, an official responsible for information systems in one agency granted a waiver of safeguard provisions. A manager in data base administration brought to his attention that this seriously compromised security over personal data in the files. The agency decided that processing should continue in order that the schedule should not be "slipped."

Defining responsibility for security administration

At many agencies, organizational responsibilities for security administration were not clearly defined. Usually, security responsibilities were fragmented or overlapping and not coordinated. This resulted in an overall lack of control of computer data security management.

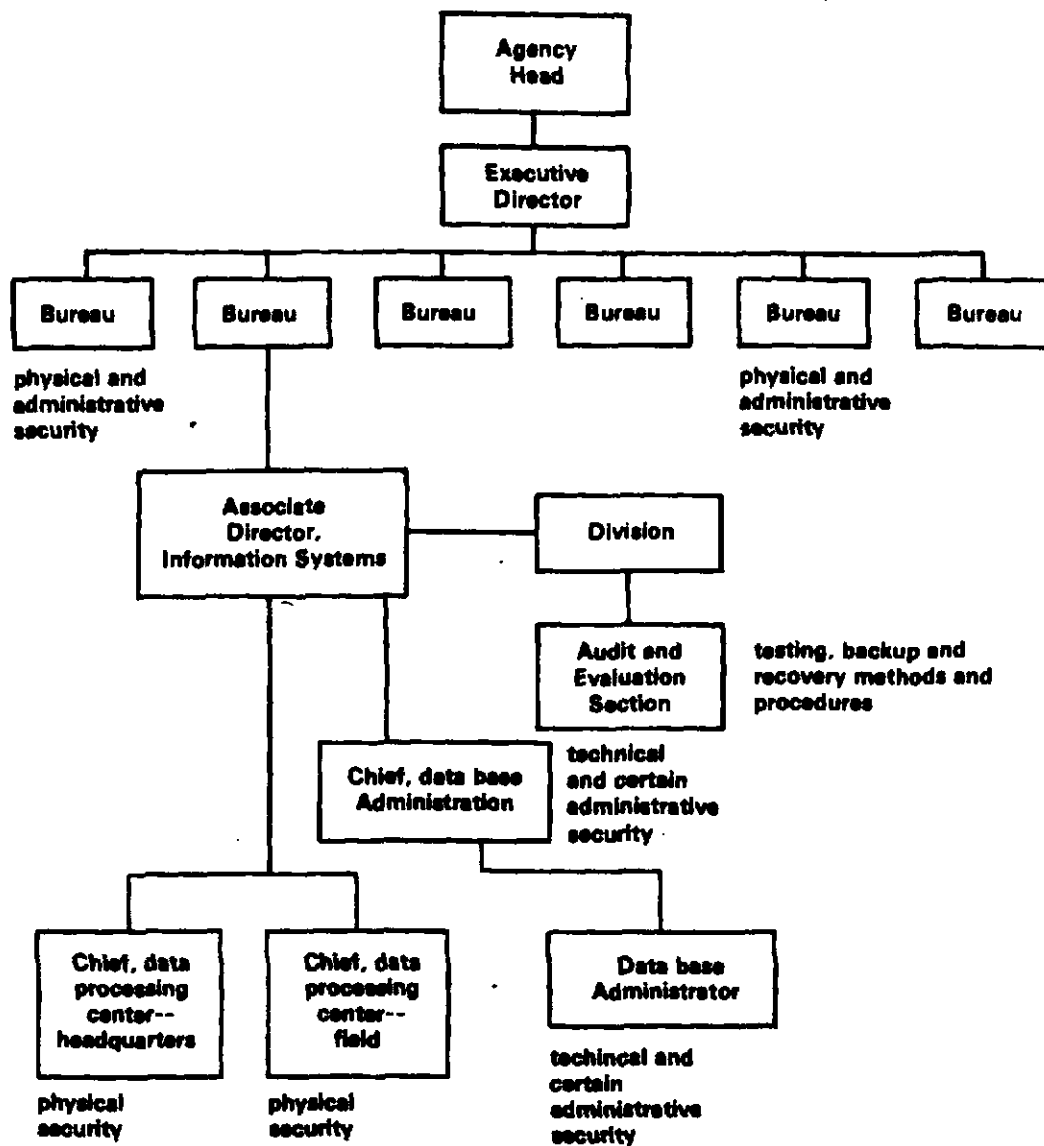
Only 4 of the 10 agencies we reviewed had clear, overall computer data security administration responsibility placed within a single organizational element. In five other agencies security responsibilities were defined to only a

limited degree and they were shared by two or more organizational elements. One agency had not defined security responsibility within its organization.

Because three different activities in one agency shared security responsibilities, and the roles of individuals were undefined, delays resulted in implementing the computer security program.

In the one agency where we did not find computer data security responsibility defined, we identified at least three organizational units that believed they had some responsibility for data security. No one organization or official had been charged with overall security responsibility, and the management position above these three organizational units had been vacant for 2 years. Under these conditions, one organizational unit was waiting for another to act on security, and security measures were implemented only if requested by users. As a result, not much had been accomplished.

An example highlighting another agency's organization with security responsibility weaknesses is illustrated in the organization chart below. The agency did not have a centrally directed security administration function. This agency's data base of personal records was one of the largest maintained in the Federal Government.



In this agency, responsibilities for computer security were spread among several organizational units and, for the most part, were ill-defined. Formal written responsibilities for technical and certain administrative security had been issued for the headquarters data base administrator; such responsibilities of the other, subordinate units were informal and unclear. Responsibilities for physical security appeared to overlap. The responsibilities of the regional office users were undefined.

Three bureaus had some interest or responsibility for administrative and physical safeguards at the field data processing center. One bureau which had agency-wide personnel and facilities management responsibilities issued guidance on matters such as personnel clearance, control of access to critical areas within facilities, and communications. Another bureau that maintained data bases at the field computer center exercised responsibilities for physical and administrative security pertaining to that data. The third bureau issued certain directives on physical and administrative security pursuant to its line management responsibility for the agency-wide information systems and data processing operations at the two centers. Potential for conflict existed because responsibility for administering systems security generally was poorly defined; technical security was formally defined only to the headquarters data base administrator in the organization.

Officials of this agency acknowledged these organizational weaknesses as well as other weaknesses which were not conducive to an effective computer data systems security program. Stimulated by an interest in our survey, they recommended that an ADP users group set objectives for and design an agency-wide data security system and a program that would encompass identification of responsibilities for security.

Conclusions

The organizational structures that we observed were for the most part inappropriate mechanisms to achieve the awareness, planning, implementation, and feedback necessary for effective management control over computer security. The prevalence of these conditions to a large degree is causal in the existence of the other problems addressed in the following chapter of this report.

Department and agency heads should reallocate resources and assign priorities to establish computer data security administration as a staff function independent of and monitoring the ADP line organizations and their security responsibilities. This function should, in fact, support all line management using sensitive data at appropriate organizational elements including field installations and the national office. The arrangement should create the medium for effective management control of programs to protect personal and other sensitive computerized data.

SECURITY MONITORING AND REPORTING

The overall effectiveness of a security program cannot be assured unless it is continuously monitored and weaknesses are reported. Popular theories of management control emphasize that feedback is the last step in the process; it is the step which "closes the management control loop."

Procedures and implementation

OMB's directives and NBS's Federal Information Processing Standards Publications prescribe that for personal or other sensitive data agencies should make a designated individual responsible for examining installation security practices and measures. He should consider both internal uses and the authorized external transfer of data, reporting any risks to the relevant management authority. The organizations should designate individuals responsible during each processing period (shift) for insuring that the policies for protection of data are enforced. We endorse the concept of monitoring and reporting and urge its incorporation into security programs covering personal and other sensitive data.

We found that most agencies did not perform active monitoring and reporting on the (1) status of computer data security programs; (2) adequacy of safeguards for new or changed systems; (3) implementation and effectiveness of existing safeguards for computer hardware, software, and data; and (4) violations of security standards or procedures.

Many of the procedures and reports we did identify were focused on data processing operations or limited to only physical security problems. Three agencies had only limited procedures for conducting reviews and reporting risks or violations. At least five agencies did not have any security reporting procedures.

We could not find any reporting being done in six agencies although some had procedures requiring it. One of these six agencies did have a contractor address security problems as a part of its reports on operations.

We noted several reasons given for monitoring and reporting not being done: (1) management never requested it be done, (2) agency procedures did not require it, (3) the agency's computer security program had not been sufficiently developed, and (4) adequate staff was not available.

An example of the monitoring and reporting personnel being spread too thin was in an agency where responsibility for monitoring security effectiveness had been assigned to the systems security administrator. Considering that this agency had more than 290 different systems, of which about 80 contained sensitive data, very little actual monitoring had been done.

An example of reporting procedures which were inadequate to cover day-to-day operations was the visit of an ADP official to the computer site once a week to evaluate ADP operations and security. No formal reports to higher management were required or prepared in this instance. Reporting was limited to oral discussions of his findings with the head of the ADP division.

Test penetration of systems is a tool to be used in monitoring the security effectiveness of a system. Agencies generally were not using this means of testing technical security measures at the time of our visits.

In a test penetration conducted in 1975, an employee of one agency was able to obtain access to the system's automated password file and increase his system privileges. As a result of that test, procedures were changed so that the automated password file was protected by technical safeguards. Further independent test penetrations to try to crack the computer system had not been done recently because the security administration believed that top management would not incur the expense of independent tests and because present internal resources were too limited. The data on file is sensitive business data of companies regulated by this agency.

A test penetration of a system of another agency was attempted in February 1976 by an outside activity which

was successful in gaining access to the computer operating system from a remote terminal. This allowed full access to the agency's sensitive data files. Action was initiated to strengthen the security but had not been fully implemented and no further test penetrations were made.

One agency demonstrated to a contractor that adequate protection was not provided for clients' data. This agency obtained access to a password file and conducted penetrations into the contractor's data base, using the agency's access terminals. It obtained data belonging to another customer of the contractor. The agency then shocked contractor officials by providing them with the data obtained. The contractor quickly took corrective action by generally improving its security and establishing safeguards; i.e., badge identification, visitor escort, closed circuit TV, technical control for password access protection, audit trails, and other security measures.

We did not find any other instances of test penetrations having been conducted.

Security monitoring by operating personnel

A supplement to the agency's dependence on monitoring and reporting by an independent security administrator, considering limited resources, would be security evaluations by data processing operating or user groups. This is because security is a personal responsibility; it extends to all levels; to anyone who has custody or access to data, regardless of who has responsibility for administration of the program. At least five agencies did not have program or computer operating personnel monitoring computer security; two others had the data processing operating function evaluating security but to only a limited degree.

Conclusions

Management control over protection of data requires feedback on the effectiveness of all aspects of the computer data security program. We found generally inadequate attention by management to monitoring computer security in their organizations, and inadequate interest in how security measures were working. We conclude this from noting the absence of provisions in several agencies for monitoring and reporting and from the evidence we found that several agencies were doing little, if any, reporting to management.

Department and agency heads should designate personnel to monitor compliance with their computer data security procedures and establish adequate reporting of this monitoring function. This function should be broadly defined so that those charged with monitoring have the latitude to look beyond prescribed elements in a security program and are encouraged to exercise initiative in recommending improvements to management. This is especially important since, as we have pointed out, we did not find what could be considered to be a comprehensive computer security program.

When these technical safeguards have been implemented, test penetrations of systems should be conducted on a periodic basis, to determine the reliability of controls.

CONCLUSIONS

OMB issued Circular A-71, TM-1--on Security of Federal Automated Information Systems--after completion of this review. The circular requires action of agencies' top managers which could contribute greatly to correcting many of the computer data security problems addressed in our report. The circular is directive. It is also quite comprehensive. It requires agency heads to report on their plans to comply.

Specifically, the circular promulgates policies and responsibilities for the development and implementation of computer security programs by all executive departments and agencies: it further addresses the general requirement for agencies to implement a computer security program; it establishes specific requirements for the development of management controls to safeguard personal, proprietary, and other sensitive data in automated systems; and it defines a minimum set of technical controls to be incorporated into each agency computer security program. (See app. IV.) Therefore, it sets an appropriate framework for agencies' initiatives to correct their data security problems.

RECOMMENDATION TO OMB

We view a leadership role by OMB as vital to maintaining the momentum that Circular A-71 should impart to computer security in Federal agencies. We are concerned that agencies do not lose sight of the stated purpose of the directive, i.e., that agencies develop and implement computer security programs with a scope to protect personal,

proprietary, and other sensitive data. The circular further addresses certain specific technical requirements. Accordingly, we see a critical need for OMB to follow up on the circular's requirement that agencies prepare and submit plans for compliance.

We recommend that the Director of OMB arrange for independent reviews by persons knowledgeable in computer security of the plans of departments and agencies responding to Circular A-71. OMB should critique agencies on the adequacy of their plans for computer security using the findings and recommendations to heads of agencies contained in each chapter of this report as well as the requirements set forth in Circular A-71.

RECOMMENDATIONS TO HEADS OF DEPARTMENTS AND AGENCIES

OMB Circular A-71, Transmittal Memorandum No. 1, holds potential for greatly improving the computer data security posture in Federal departments and agencies. However, we have shown that at the time of our review, agencies had not taken full advantage of the extensive guidance published previously by OMB, NBS, and other sources. (See apps. I and II.) Hopefully, OMB's new Circular A-71 will have more effect because of its directive nature and its reporting requirements (for reporting requirements see Section 8, OMB Circular A-71, TM-1, at app. IV).

To enhance the quality of agency effort in complying with the policy promulgated by this circular, a vigorous approach will have to be taken by the top managers themselves. The circular requires agency heads to assign responsibility for the development, implementation, and operation of a computer security program. We believe it is critical to the effective discharge of this responsibility that the tasks here not be merely delegated to existing resources in computer operations.

We recommend that heads of all departments and agencies:

- Establish an automated systems security administration organization with independence from computer operations. This organization should report directly to or through a principal official who reports directly to the agency head and it should have authority to discharge the enumerated responsibilities of agency heads as outlined in OMB Circular A-71, TM-1.

- Develop comprehensive computer data security programs in compliance with OMB Circular A-71 from the total systems perspective--ensure that they provide for security of data in all media and in all stages of the data life-cycle--and consider the need for controls from the perspective of all possible security threats at all locations involved with the agency's data.
- Assign to a specific group in the agency the task of ensuring that comprehensive computer data security plans and programs as developed will be documented, written, and disseminated to all activities and locations involved with the subject data, and that responsibilities for all provisions be clearly delineated. This definition of responsibility should encompass provision for implementing plans and programs further required of subordinate activities.
- Require that security programs include a provision for monitoring and reporting to top management on the status and adequacy of the program, and evaluate its implementation and the effectiveness of safeguards, procedures, and other instruments of the program.
- Anticipate training and indoctrination needs for raising expertise to the level required to implement requirements of their programs and of OMB.

OMB's COMMENTS

We provided copies of our draft report to and discussed it with OMB representatives. They indicated that our examination of the status and effectiveness of computer systems security programs was highly beneficial. It provided information and recommendations which would be used and followed up in their own assessments of federal agencies' plans to comply with their Circular A-71 and other requirements.

OMB is placing a high priority on efforts over the coming year to improving security programs in agencies and has organized a task force to accomplish reviews of agencies' plans. This effort is coupled with OMB's broader concerns for improving controls in agencies over fraud and abuse. OMB indicated that attention by agencies' inspector general functions will be focused on correcting these matters in

recognition that they are important responsibilities of agency and department heads.

OMB expressed some concern that our recommendation for organizing a highly placed computer security administration as a staff function, independent from computer operations, might cause difficulty with the agency head's span of control. That is, too many functions are now competing for top level attention and this would add one more. We recognize this problem and intend our recommendation to be sufficiently broad to allow each agency maximum flexibility in its implementation in a wide variety of agency organizations.

We agree with OMB that elements of this security function such as monitoring, inspection and audit could be placed under the emerging inspector general function. But we see the need for identification of a focal point at a high level, independent from responsibility for computer operations, to develop and oversee an automated systems security program. The security program itself should be promulgated by a directive and guidance issued by the agency head.

CHAPTER 3

SELECTING AND IMPLEMENTING SAFEGUARDS

We found that agencies generally selected computer data security safeguards intuitively rather than on a formal and disciplined basis which would consider cost-effectiveness relative to degree of data sensitivity and risk. Furthermore, safeguards required in many cases were not functioning adequately to provide acceptable levels of protection.

In this chapter, we evaluate agencies' methods of safeguard selection. We also discuss their management of policies, controls, and methods for restricting access to data base information and computer facilities.

RISK ANALYSIS AND SAFEGUARD SELECTION

Most agencies had not adopted a risk management concept to select economically feasible safeguards for protecting sensitive data. At certain levels in some organizations, however, steps in that direction had been taken.

In this report, we use the terms "risk management" and "risk analysis." The distinction between the terms is minor. Risk management is a concept which recognizes that complete computer security is impossible to obtain. Risk, however, can be managed to an acceptable level when the degree of data sensitivity, vulnerability, integrity, and costs are accorded the appropriate weight. Risk analysis is the application of steps in an analysis which considers data sensitivity, vulnerability, and costs to a computer facility or computerized system, periodically, to select economically feasible safeguards. When implemented, these safeguards should then enhance management of risk to achieve acceptable levels.

The NBS Federal Information Processing Standards (FIPS) Publication 31 outlines the steps of risk analysis, for a facility, generally as follows:

1. Estimate the potential losses to which the ADP facility is exposed.
2. Evaluate the threats to the ADP facility.

3. Combine the estimates of the value of potential loss and probability of loss to develop an estimate of loss expectancy.
4. Select from safeguard alternatives on the basis of cost justification.

We heartily endorse this format, but we stress that although safeguards will be evaluated and implemented at facilities, risk analysis should also be applied on the broader scope of a total data system. This is because protection of data in systems usually always involves coordination and integration of activities at a number of locations. For example, "hard copy" data is frequently mailed from one location to another. In a more automated sense, the use of remote terminals to communicate with a computer is common.

One of the agencies we reviewed had made a noteworthy effort to apply risk analysis to assessing need for improving safeguards and controls in its data systems. The steps this agency set out are tailored to its specific organizational needs and appropriately address criteria for selection of economically feasible safeguards. The agency's steps, summarized, are to:

1. Determine the sensitivity of data.
2. Analyze vulnerabilities and identify specific weaknesses of the computer system.
3. Determine risk--i.e., using vulnerabilities as a basis, identify perceived threats along with an estimate of their chance of occurrence.
4. Identify safeguards that could be used to minimize the threat and determine costs for each safeguard.
5. Select the most cost-effective safeguards to reduce the threat to a minimal acceptable level.

A number of variations on risk analysis methodologies exist. Clearly this is not an exact science. In some applications it may not be feasible to generate more than rough estimates; however, the value of disciplined attention to managing risk is crucial to data protection.

Many managers in agencies below the upper levels and technicians recognized the feasibility and desirability of the procedure, but cited, most often, lack of resources and lack of needed top-management priority as the reasons for not accomplishing risk analysis.

One excuse we encountered for not adopting risk management was that it is too theoretical and imperfect. These objections were usually centered on the difficulty of determining the degree of data sensitivity, especially by the technique of determining the cost to the organization of having data elements compromised. We recognize that these details sometimes involve making best estimates and indefinite value judgments. We contend, however, that risk management is an adaption of the widely known and accepted problem solving process which always requires a large amount of initiative and some innovativeness but for which there is no acceptable substitute. The least acceptable of the alternatives is doing nothing.

In selecting safeguards, agencies must systematically perform and document (1) definition of the problem, (2) identification of alternatives, (3) evaluation of alternatives, and (4) selection of an alternative. The concepts in NBS guidance have gained wide acceptance among computer security experts in Government and private industry, but they are not being applied in practice.

Risk analysis is an essential first step in the development of an effective computer security program. OMB's directive on new systems containing personal information (see p. 55) requires that risk analysis be applied by all agencies. Agencies must retain the details in files. These requirements are explicit for new or altered systems with personal data and are otherwise implicit for systems with any form of sensitive data. Very little was being done to comply.

--Only one agency of all those we surveyed had a risk analysis procedure and used it to select safeguards. The System Security Administrator performed a systematic vulnerability, threats, and risk analysis based on his adaptations of NBS standards (FIPS Publications 31 and 41) and the methodology taught at the Department of Defense Computer Institute.

--Another agency had a requirement in its "Structured Action Plan" that a risk analysis be performed by the

systems security officers of each headquarters control component, regional office, and field office which processes or uses personal data. For one large data system only, a study of computer-related crime vulnerability was accomplished and reported. This study was not comprehensive in the risk analysis sense, because all protection alternatives were not costed.

--The Privacy and Security Officer of one agency had implemented certain interim safeguards. Although no agency procedures existed for performing a risk analysis, she was beginning one for the entire ADP division. She had no projected date for completion of the analysis because she anticipated budget restriction problems.

--During the course of our visit to one agency, a person was designated to develop risk analysis procedures. Previously, that agency had not developed procedures for, or performed, risk analysis.

--The Chief, Data Processing Operations Branch, in another agency which had not undertaken risk analysis had recommended to the head of the Security Division that a risk analysis program be implemented. He said that the Security Division had issued no policy as a result of his efforts.

--The department level of an agency we surveyed had an "ADP Physical Security" document that set out the general requirement for risk analysis but did not provide specific guidance. The agency had not complied with this requirement. We were told that only one bureau within the entire department had conducted a risk analysis.

These examples cover the extent to which we found attention to risk management in agencies we surveyed. The remaining 4 of the 10 agencies surveyed had no procedures and had not taken any action on risk management.

SAFEGUARDS

The managerial and administrative aspects of agency measures to restrict access to data and computer facilities were neglected. Many trained and knowledgeable technicians

and lower and middle level managers in agencies we reviewed had implemented various security measures, but their efforts were oftentimes piecemeal. Support and attention of upper management levels was lacking in many instances discussed in this chapter.

We looked for policies, measures, and procedures aimed at protecting specific data. Because of resource limitations, we did not test controls that agencies selected and implemented, but rather evaluated the management direction given to development of adequate protection safeguards.

Administrative considerations

Administrative safeguards or procedural security establishes activities which are functions of human authorities, judgment, and decision processes. Through these actions or procedures, management can directly influence the effectiveness of its computer security programs. Additionally, management influence and direction should extend to the administration of technical safeguards. Technical safeguards include software features built into the computer systems to help control access, limit user privilege, and maintain program integrity. Also, controls or activities provide physical protection over access to data and computer facilities. The latter two areas are discussed in the succeeding sections of this chapter.

Controls over information storage

A program to provide security for data must provide adequate safeguards for all forms in which the data resides in a system, from its collection to its dissemination to the user. This means that the security program must provide for security of (1) the source documents, (2) on-line and off-line computer media storage, (3) the data during processing and the vulnerable transmission stages, and (4) the data output on user media.

We noted instances of unsatisfactory computer media storage. For example, a security assessment conducted by one agency found that 4,000 magnetic computer tapes were stored outside a tape library vault. Active data tape files were maintained in computer rooms while active program tapes were stored in a scheduling area. The agency recognized that the lack of the additional security provided by the vault increased the potential for sabotage, alteration,

and/or theft of data or a tape. Their study also disclosed that any programmer could request any tape in the central office tape library. With knowledge of a tape's format and record layouts, any tape could be altered. Also, any person could alter tape retention records to prematurely release tape files, and tapes were not being erased before being sent off-site. As a result, data could be read by the next user.

It was disclosed that the tape librarians at the data operations center had access to backup systems and tapes prior to transmission. Thus, at that agency the records were not properly controlled so that alterations for personal reasons or monetary gain was possible. The agency had not performed a risk analysis to demonstrate a low level of vulnerability and probability or that safeguards were not cost-effective: rather, the above conditions simply developed without adequate management attention.

Background investigation

Untrustworthy or dishonest employees who have access to systems (i.e., designers, programmers, and operators) present the major threat to sensitive data in an automated system of records. This is so because system penetrators must possess (1) programming skill, (2) understanding of a sometimes rather complex system, and (3) knowledge of the limitations that occur in the design and implementation of the system.

In a prior report, 1/ we supported the Internal Revenue Service (IRS) regulations which recognized that a security investigation program should be designed to provide information about an individual's background commensurate with the degree of responsibility and trust imposed by the position to be held. Applicants for specified positions in the agency and those on whom investigations uncovered derogatory information received an extensive character investigation. These specified positions included all computer personnel positions.

We believe the above procedures were adequate but that periodic reinvestigations should be conducted as it is for clearances for national security information. The agency

1/"Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, Jan. 17, 1977).

was not doing this for computer personnel to ensure that the activities of the individual employees were such as to warrant the Government's continued trust.

Our present review disclosed that most agency employees with access to sensitive data, whether they be computer operating personnel or users of terminals and sensitive data, receive only a National Agency Check (NAC) or an NAC and Inquiry. This procedure is not as extensive for determining trustworthiness and job suitability as a full field investigation. Also, the NAC and the NAC and Inquiry do not require periodic followup investigations; the full field investigation does. We believe that the followup is necessary for personnel working with personal and sensitive data on computers.

Full field investigations are performed only for top management, policymakers, investigators, and people having positions considered critical-sensitive. It does not include employees who have access to unclassified personal or sensitive information. There was no criteria for including in position descriptions the need for more extensive background investigations for Federal employees that access sensitive data.

We found that three agencies did not provide, through contract clauses, the requirement to perform background investigations on contractor employees who have similar access to personal and sensitive data in automated systems.

ADP security procedures in the agencies we reviewed also did not address the identification and monitoring of disgruntled employees having access to sensitive data.

Protecting the system from agency or contractor employees capable of and motivated to breach security is difficult without personnel controls including background investigations and monitoring by supervisory levels.

Training

Management cannot achieve the awareness and impart the enthusiasm to implement an effective ADP security program without adequate training.

The agencies we reviewed generally had not provided comprehensive computer security training. The training was sometimes limited to physical security, the Privacy

Act, or informal happenstance type briefings and question and answer sessions on the job. Additionally, training was not provided to all ADP systems users, particularly regional office personnel.

Half of the agencies we reviewed had conducted some computer security training. In one agency, this consisted of a 2-1/2-hour course given in 1975. The course was given to personnel of only one of the three bureaus involved in the computer system, and was not focused on computer security--it only included some security exposure. In another agency, about half the users received a 2-hour presentation in 1977. There had been no other formal training. Regional office terminal users on one occasion were given a security orientation. Presently, all new employees of this agency working with ADP are given a security orientation. Training in another agency was limited to a training session on procedures for handling material and to a request that employees read the security manual. They did conduct training on the Privacy Act. One agency has an "interim training procedures" manual; however, no centralized training was conducted. New employees at only one of the agency's several data centers we visited were briefed on ADP security. Existing employees received security training on the job via informal contact with supervisors.

Computer security training in the other five agencies we examined, where it existed, consisted of less than that described above.

Contractor security

If contractors are involved anywhere in the collection, storage, maintenance, or processing of agency data, and their operations do not provide the same adequate level of security required of agency internal operations, the agency's data is not adequately protected.

Most agencies that used contractor ADP services did not review contractor security, and several of the agencies we surveyed did not even define security responsibility adequately in contracts. Some specific examples follow.

--One agency that relied heavily on contractor data processing support for one of its major programs which contained sensitive data did not have a program for assessing contractor security effectiveness.

Agency personnel had neither visited the contractor's data processing facility for security purposes, nor tested the effectiveness of security by other means.

--Officials of another agency informed us that they were reluctant to store records in a contractor's computer facility because of a lack of adequate technical system safeguards. A general agreement merely required the contractor to comply with the Privacy Act and the rules and regulations pursuant to the act. We found that the contractor was not specifically required to establish audit trails and password or program controls (discussed in following sections). In fact, the contractor had not established safeguards to adequately protect data processed on its computer, and the contractor's computer facility officials admitted that by inputting a user's identification number and random tape numbers, it would be possible for anyone to randomly sample and read data tapes of other computer users.

--At a facility we visited, the contractor/operator disclaimed any liability for disclosure of sensitive data. A contractor official indicated that emphasis is placed on protection of computer hardware and facilities; however, the contractor does not provide controls for data protection.

- - - - -

In a separate but related study requested by the Chairman of the House Subcommittee on Government Information and Individual Rights, we reviewed efforts to implement subsection 3(m) of the Privacy Act at 10 Federal departments and agencies and about 60 Federal contractors. The purpose of subsection 3(m) is to provide appropriate safeguards when contractors are handling personal information subject to the act. We concluded that the improper use of such information, to the extent it can be determined, has not been widespread, but if so, it could cause much harm. (See "Privacy Act of 1974 Has Little Impact on Federal Contractors," LCD-78-124, Nov. 27, 1978.)

Audit trails

Generally, audit trails should be employed so that security administration can monitor computer data use and

the system security features regulating integrity. Audit trails can be designed to meet unique requirements for the level of security appropriate in a particular system. They should be designed to record who had access to what data. Depending on the level of detail desired, they can identify such things as the file, the record, or even the data element accessed and what transactions were performed.

Most of the agencies we reviewed did not give attention to achieving an audit trail capability. At least 6 of the 10 agencies did not account for accesses to data or did not provide for a capability to reconstruct, if needed, such an accounting for data use.

In some cases, absence of an audit trail would make safeguards less effective. For example, one agency provides that a computer will disconnect a remote terminal after three unsuccessful attempts from it to gain access, e.g., by using invalid passwords or log-on procedures. However, no audit trail or other means existed to identify these unsuccessful attempts.

Not all of the agencies where we found audit trails used them for ADP security purposes. For example, one agency does collect on tape the entire record of every individual query for data. However, the tape is used as the source for a daily summary report of communications network activity. The data on the tape is erased after one day and the tape is not used for any kind of security review. In this case, there were no controls to limit the number of attempts that could be made to improperly access data.

Another agency compiles a daily transaction tape which contains all the detail associated with each access action, i.e., password, user ID, terminal, transaction tape, etc. However, the tape is not reviewed for security purposes; it is used only for recovery of operations on a backup computer if one computer fails.

Passwords

We found the use of passwords to be widespread, but password administration was generally poor. Only two agencies we reviewed did not use passwords at least to a limited degree. The agencies did not conduct a risk analysis in each case that would enable them, or us, to

judge whether the use or absence of passwords was appropriate to their data files.

We advocate the periodic changing of passwords to provide for continuing protection in the event of undisclosed compromise. We found examples of password systems in use for security purposes, however, where the passwords were not changed. This was the case in several agencies. An official at one of these agencies advised us that the agency planned to change passwords at least once a month, but those plans were not implemented. In one system of records, passwords had not been changed for at least 3 years.

In three agencies, more than one person using remote terminals had identical passwords for access to sensitive data. This results in a weakness in controls over potential system penetration (unauthorized access, modification, or destruction of data) and a lack of accountability for system use. We noted as many as 10 people or more using the same passwords or user identification codes in one instance.

When passwords are used and typed out by a printer, a technical control should be employed causing the password line to be overprinted, thus making it illegible. We observed an instance where this provision was made but the control was not working. The result was that passwords appeared legibly on documents.

In another instance, individuals did not appreciate that the passwords they were using were for security purposes. We noted that at one agency, employees were using other peoples' passwords for convenience, and were writing their passwords on documents which were not kept secure. Also, punched cards showing printed passwords were displayed on a wall.

Establishing a password system is not enough to provide an ADP security measure. The system must be monitored to preclude the undesirable conditions described above from degrading effectiveness.

Program control

Computer security should include controls to restrict access to and protect the integrity of computer programs

and provide copies only upon specific authorization. The objective is to isolate the programmers from the system to reduce the potential for unauthorized program modification.

We did not find any measures for program control in two agencies we surveyed.

--At an agency maintaining a large data base, computer operators were not restricted from adding new versions of computer programs to the program libraries. Also, any programmer could request any tape in the computer center library without security control, and anyone could make minor modifications to programs at anytime without supervisory authorization.

--Another agency could not identify who made changes to computer programs and what kind of changes were made. The agency could not determine how many active and current programs were in the library. Because the agency maintained many obsolete versions, erroneous processing might result, and there was potential for illegitimate functions' being processed.

Quality assurance

During the conceptual, design, and preoperational phases of a new system development, controls should be evaluated. This should be accomplished to ensure that adequate safeguards are built in at the beginning of a system's life cycle. Some agencies had some form of quality assurance testing, but half of the agencies we surveyed did not provide any measures to build in security safeguards during the development of new systems.

One agency had established a requirement to perform quality assurance testing, but we were told that nothing was being done because of staffing and workload problems. A reason given by an official of one agency for not conducting quality assurance of security in new systems was concern with overriding priority of timeliness in getting the systems in operation.

We found that only four agencies had either the security administrative function or internal audit organizations participating in quality assurance of security in new systems. In one of these agencies, preoperational reviews of the adequacy of ADP security controls were conducted. Internal audit was informed of development activities before a

proposed system got into the acceptance testing phase. Another agency conducted "preinstallation" reviews after programming but before conversion to the new system to evaluate the system test plan, the internal controls, and the general management approach to the system.

One agency had a quality assurance section in its organization specifically detailed to pre-edit all data prior to input to ensure validity. The agency's Information and Management Division was responsible for formulating security applications for the agency's systems branch as well as creating new systems and enhancements to systems. Yet, another agency's internal audit organization was involved in the design and development of new systems with a view toward security safeguards.

Separation of duties

A procedure to promote computer data security is to make collusion necessary in order to violate security of a system. In practice, all people involved with the system should be able to get only enough information to do their job, and no more. Where suited to the system needs, the transaction-oriented system (where the user only inputs and receives specific data) is more desirable for control purposes than having a more interactive system. An example is the airlines' ticket reservations system. Reservation clerks can only query on the availability of seats and can sell seats. They cannot adjust passenger seating or change flight schedules.

The principle of giving people only enough information to do their job should be extended to wherever possible during the design, implementation, and operation of a system. Designers should not receive sensitive data elements if they do not need them, programmers should not have access to data if they do not need it, and users should not be able to change programs.

We found that the concept of separation of duties for control purposes was adopted to a limited degree in only four agencies. This is to say that these agencies had provided for separation of duties in from none to only a few isolated instances; the concept was not used on a widespread basis within any of the agencies.

Technical safeguards incorporated
into systems

Technical safeguards are generally software features incorporated into systems design and working with procedural safeguards to help control access, limit user privilege, and maintain program integrity. We believe that the low level of concern for computer security exhibited in most of the agencies in this review--i.e., lack of programs or use of risk assessment--makes it unlikely that the use of the more sophisticated technical controls was widely or adequately considered. Therefore, our discussion of technical controls which were potentially available is intentionally very selective.

We recommended in a previous report 1/ that such selected controls "built into the computer" be employed in an agency using particularly sensitive information.

Controls over access to personal
or other sensitive information

Access to specific data files, records, and data elements within records can be achieved through software controls. We believe agencies should incorporate these controls in the development of their application software. In cases where only a segregable portion of a data file is routinely accessed by the specific set of users, supervisory or second party intervention should be required to access other more sensitive data. Also, segregation of files can be planned to limit access to the total data base.

The IRS agreed to adopt software controls of this nature in its proposed new system. Access to the preponderance of taxpayer information needed by IRS employees to perform the audit and collections function would be confined to the geographic district to which the employees are assigned. Therefore, a district or local office employee would be restricted to the access of an average of less than 2 percent of the total taxpayer accounts.

1/"Safeguarding Taxpayer Information--An Evaluation Of The Proposed Computerized Tax Administration System," (LCD-76-115, Jan. 17, 1977).

Data terminal user access controls

We stated earlier that we found passwords widely used, although password administration was generally poor.

We believe that when justified by the sensitivity of data and other factors, agencies should consider terminal and employee profiles for use in conjunction with passwords. Such profiles are tables maintained on the computer system that contain the information necessary to (1) identify authorized terminals and users of the system and (2) restrict those terminals and users to executing only authorized commands. This control is in accord with the concept of separation of duties and the concept of command codes described below.

Controls over assignment and use of command codes

Command codes activate computer routines for the processing of data and inquiries. Each code performs a specific function in relation to the transaction entered and the data maintained in the system. The number and combinations of command codes an employee is permitted to execute determines the capability of the user to process or obtain data from the system. We believe that this safeguard should receive wide consideration as a means of limiting privileges given a system user.

Physical safeguards for data and facilities

The need for physical security against such hazards as fire, sabotage, and theft is well known and has been examined in our previous reports. Our present discussion of physical security is intended to be very selective and includes only two facets as they particularly relate to data protection and backing up the systems which process it. The first concerns physical access.

Controlling access to the data processing facility or its individual component resources, is the most obvious means of protection and the facet of computer security which received the most attention in agencies' facilities we visited. The second facet of physical security we address is backup and recovery for operations in the event of destruction or compromise of system data, programs, or computer hardware.

Physical security procedures

We found examples of ineffective physical controls which could be traced to (1) the lack of overall ADP security programs, (2) fragmented security responsibility, and (3) generally weak management control, i.e., limited monitoring, reporting, and auditing of security. However, because of the sometimes obvious and passive nature of safeguards which control access to facilities and component resources, these forms of safeguards have received the most attention in the agencies we surveyed.

We noted instances where physical access controls had been instituted but did not receive followup. For example, a television camera was set up to observe physical access to a data processing center, but it was not being watched by anyone. In another case, an intrusion detection alarm was set up around one of an agency's data processing centers, but the agency's Associate Director for Data Processing told us that it had not been in operation for up to a 3-month period. Agency officials said this condition persisted because the alarm system was not regularly tested.

We found that even the most obvious precautions were not always taken. For example, in one agency computer printouts containing sensitive data were left carelessly strewn throughout a user's facility or were left on desk tops in areas without access control.

Backup for data

Agencies' provisions for duplicate data or reconstruction of data in the event of loss or destruction were good. All agencies we surveyed had given this matter attention and had reasonable backup. The "grandfather, father, son" concept--retaining master files updated by data for three or more generations of transactions--was widely adopted.

In some cases, however, backup data files were in such proximity to primary data storage that they provided for continuity of operations in the event of accidental erasure, but not in the event of a disaster such as a fire, explosion, or flood. The vulnerability of many Federal systems to such

disasters and some devastating results which have occurred are treated more thoroughly in one of our prior reports. 1/

Backup for hardware

Agencies had not provided for backup of computer hardware as adequately as they had for data. Whereas data backup is elementary in the training and day-to-day functioning of ADP operating technicians, hardware backup requires more management attention. Four of the 10 agencies we reviewed had made reasonable provisions for continuity of operations in the event of hardware loss. One other agency had limited provision for hardware backup.

Admittedly, the problems with hardware backup are sometimes perplexing. One reason frequently cited was that hardware compatible and adequate for the systems as designed and used is not feasibly located, or in some cases, does not exist. One agency informed us that only one system compatible with its system exists, but the owners do not have enough peripherals to support the agency's operations.

Reasons for no hardware backup provisions were discussed with the Systems Security Administrator in another agency who was organizationally located within ADP operations. He informed us that while he had pointed out to various superiors the need for hardware backup, he was told that efforts to arrange backup would have to wait because of higher priorities. He also said he knew of no other organization that could provide the same computing power and computer configurations to permit it to operate at full capacity in an interactive mode. However, we found that the Systems Security Administrator had not discussed the matter with the agency's hardware company representative. We discussed this matter with the hardware representative and were informed that arrangements could be made to operate the system in a degraded mode. The same information would presumably have been made available to the Systems Security Administrator. Planning for such contingencies should be formalized.

1/"Managers Need To Provide Better Protection For Federal Automatic Data Processing Facilities," (FGMSD-76-40, May 10, 1976).

THE HEW TASK FORCE REVIEW

The significance of the HEW Task Force review (see p. 1) was the disclosure of how far component agencies had fallen short of implementing the HEW standards published to implement OMB directives and NBS technical guidance. Agencies had not adopted and monitored comprehensive security programs adequate to protect the confidentiality and integrity of sensitive data maintained in their computer-supported information systems.

The HEW review team found that no departmental component reviewed had the real and continuing support of management necessary to assure the creation and maintenance of a viable program of systems security. Although some agencies within HEW had published some form of structured action plan at the headquarters level, regional offices or staff offices had not implemented viable plans. Because top management in HEW component agencies was not implementing and enforcing the Federal or departmental standards, lower level managers (and in some cases even system analysts) were attempting to determine, without adequate direction, the level of security and specific safeguards, if any, for their systems.

Some of the areas of computer data security weakness cited in the task force's reviews of computer applications and facilities in HEW components were lack of (1) risk analysis, security planning, and implementation (2) contingency, disaster, and emergency planning (3) facility and data access control and (4) training.

The Task Force's evaluation of departmentwide non-compliance with HEW's published computer security standard was confirmed on a broader basis by our review of a Government-wide sample of agencies.

Major recommendations of the task force were that HEW components (1) develop and manage a computer systems security program, (2) ensure that all decisions regarding safeguard selection are based on a complete risk analysis, (3) appoint an ADP systems security officer in the Office of the Secretary, (4) ensure adequate management controls over systems development, and (5) develop contingency and disaster plans.

CONCLUSIONS

Agencies we reviewed generally had not given attention to risk management in their security procedures. Only two

out of the ten agencies had completed an analysis of data sensitivity, vulnerability, and costs to select cost-effective safeguards. In one case, the study was not comprehensive in the risk analysis sense because all protection alternatives were not costed, and it pertained to only one of several systems in the agency.

A good deal of attention had been given by technicians and lower and middle level managers to the obvious and traditional physical safeguards which could be implemented by initiatives at their levels, but they were limited by the absence of a formal computer security program for the agency. Safeguards which require higher level management decisions for administration were frequently neglected. Additionally, where safeguards were supposed to be operational, they were in many cases poorly administered or not complied with. All agencies had provided for continuity of operations in the event of accidental data erasure. However, the provisions made for backup data storage did not provide protection from disaster because of proximity to primary data storage.

In summary, the safeguards we found were, for the most part, selected intuitively. Because of this, and the lack of coordinated attention to ADP security in agencies, many "front door locked, but back door open" situations existed. The result unfortunately was often no security rather than a little security.

Department and agency heads should provide for the management of security risk in their agencies through the selection and periodic reevaluation of safeguards by the risk analysis concept. We commend the National Bureau of Standards guidelines for risk analysis to those responsible agency officials who are involved in the economic selection of safeguards. Acceptable security cannot exist without comprehensive, coordinated programs. Piecemeal selection and implementation of safeguards, lack of monitoring safeguard effectiveness and goal accomplishment, and weakness of controls agencywide, such as field office terminals and contractor operations, all degrade security to the point where it is inadequate. Management should eliminate these weak links.

Generally, we did not find training conducted which was adequate to achieve a level of knowledge in employees necessary to effectively implement present minimal security requirements of agencies. Additionally, agency development

of more comprehensive computer security programs would impose a further challenge to employees.

RECOMMENDATIONS TO HEADS OF
DEPARTMENTS AND AGENCIES

OMB requires in Circular A-71 (Transmittal Memorandum No. 1) that every agency head assign responsibility for the conduct of periodic risk analysis for each computer installation operated by, or on behalf of, the agency. We recognize that the focus on "location" stresses that no location or activity should be immune from the need to evaluate risk and select cost-effective safeguards. We stress, however, that risk analysis should be conducted from the perspective of a data system to select safeguards oriented to the total data system--to preclude uncoordinated and uncomplimentary efforts by various locations.

Therefore, we recommend that heads of departments and agencies ensure that (1) periodic risk analysis be conducted for the selection of cost-effective safeguards, from the total systems perspective, and (2) this effort in their organizations be directed and monitored by an independent computer data security administration reporting directly to or through a principal official who reports directly to the agency head.

Additionally, agencies' security plans should anticipate their increasing training needs, particularly for risk analysis, and make these needs known to the organizational level responsible for training.

CHAPTER 4

INTERNAL AUDIT INVOLVEMENT

In the agencies we surveyed, internal audit organizations were not significantly involved in assessing computer or data security programs or the systems controls needed to protect personal and other sensitive information. The root of the problem is that agency top management has generally neglected development of audit capability with necessary technical computer expertise and, correspondingly, is not committed to having internal audit participate in a significant way to controlling computer systems, operations, and resources.

Agency management has become increasingly dependent upon computer systems for information to plan, evaluate, and control its program operations and thus has reasons to be concerned about protecting this information as a valuable resource. However, agencies have been slow to appreciate the contributions independent internal audits can make toward maintaining acceptable system controls and security standards. 1/

In this context, computer security audit, to maximize its potential contribution to more effective management, must be broadly conceived. Audits should be broadly scoped to encompass protection of data and computer systems to produce the data; integrity, accuracy, and reliability of data; and operational reliability and performance assurance. 2/

In chapter 2, we stressed the importance of day-to-day monitoring and reporting by a highly-placed agency computer security function so that management could get feedback on implementation which might or could run counter to plan.

1/The Stanford Research Institute reported similar findings and conclusions from its study conducted for the Institute of Internal Audits discussed in app. I.

2/In a Government/Industry conference, discussed in app. I, broadly scoped internal audits were widely supported by computer security experts and executives who convened on the subject of audit and evaluation of computer security.

Internal audit involvement in computer security, as defined above, should go beyond providing this feedback on how established procedures are working. Internal audit and monitoring are complementary in their potential for contributing to management's meeting its computer and data security responsibility.

THE EVOLVING ROLE OF INTERNAL AUDIT

We fully support agency internal audit's going beyond the financial focus they had in the 1950s. We issued "Standards for Audit of Governmental Organizations, Programs, Activities and Functions" in 1972, which prescribed a broad audit scope to include

- reviews for compliance with laws and regulations,
- reviews to determine whether an agency is doing its job in the most economical and efficient manner, and
- reviews to determine whether the objectives of the programs authorized by the Congress are being met.

Many agencies have gone far in adopting this concept.

In a September 1977 report, 1/ we stated that some executive departments' audit organizations have avoided work in (1) computer systems design and development, (2) equipment administration, (3) specific applications, and (4) installations management. We found in our present review that many organizations are still avoiding significant work in computer security.

Federal agencies are placing heavier and heavier reliance on computers, with a proportionate increase in vulnerabilities. The consensus of Government and industry computer security experts (see p. 58) is that computer security audit, as a function of agency internal audit, should be recognized as a key element in a system of management control. Agencies fall short of making this important provision for management control.

Only one of the agencies we surveyed had its internal audit organization perform a computer security review that

1/"Computer Auditing in the Executive Departments: Not Enough Is Being Done" (FGMSD-77-82, Sept. 28, 1977).

was somewhat broad in scope and on an agencywide basis. In that case, the review currently being conducted was the first one of its kind by that organization, and it was precipitated by a serious security breach incident.

Six other agencies' internal audit organizations had conducted very limited audits. Usually, they were restricted to certain systems, or computer security was treated incidentally during a broader computer audit. In other instances, they were limited to specific areas of computer security, such as protection of financial assets or to selected cases of physical security. In the remaining three agencies we reviewed, internal audit organizations had not become involved in computer security.

Internal audit organizations should become involved in the design, development, and test phases of a new computer system as a normal part of the audit function to help ensure that adequate security is built in before a new system goes into operation. Since technical controls usually are an integral part of the whole system, and can not easily be retrofitted at a later date, these early phases in the system's life-cycle are the optimum time for control safeguards to be incorporated. Independent internal audit involvement is highly desirable to ensure that factors to enhance auditability, audit trails for security, and quality output are designed and developed into new systems. Emphasis during these stages may otherwise be on operational priorities and implementation time goals at the expense of the above goals.

Followup is then necessary by the internal audit organization after the system has become operational. This followup measure should determine if the controls have been deleted or compromised subsequent to design and testing of the system. 1/

1/OMB Circular No. A-71 (Transmittal Memorandum No. 1).

Subject: Security of Federal Automated Information Systems, became effective on July 27, 1978 (discussed in app. I). It requires that heads of agencies establish computer security programs which provide for design reviews and certification that controls meet approved security specifications. The requirements are to be applied to all new computer applications and significant modifications to computer applications. The circular also requires audits or evaluations and recertifying these controls at appropriate intervals but at least every 3 years (part 4, c and d).

Of those we surveyed, only one agency's internal audit group was involved in these early phases to a significant degree. A second agency's internal audit group had been involved in the design, development and test phases of only one system in the agency. Another had been involved in various systems but only to a limited degree. The other seven agencies' internal audit organizations had not been involved.

In the final analysis, we found that agency top management did not capitalize on the potential for independent internal audit to contribute significantly to the advancement of computer security and data protection.

INTERNAL AUDIT CAPABILITIES

A primary reason for lack of significant internal audit involvement in computer security was that most agencies' audit organizations do not have adequate personnel with ADP expertise. Officials of seven agencies informed us that their ADP capabilities ranged from no qualifications to perform indepth security type reviews to limited abilities.

We found little evidence of use of outside contracted resources to increase internal audit capability. In one instance, we were told the reason was that the audit group did not even have the expertise to specify tasks and parameters within which consultants could operate.

Our September 1977 report 1/ on the low incidence of computer audit conducted in executive agencies cited auditors' lack of technical ADP knowledge as a barrier to performing effective ADP audit by the organizations whose involvement was found to be inadequate. We recommended to heads of agencies that they develop adequate expertise in their internal audit organizations. We found that previously cited deficiencies are still prevalent. This is of increasing concern since agencies' operations are becoming heavily committed to computers, and computer technology is in a dynamic state needing constant monitoring and review.

1/"Computer Auditing in the Executive Departments: Not Enough Is Being Done" (FGMSD-77-82, Sept. 28, 1977).

DEPARTMENTAL AD HOC TASK FORCE

The use of a temporary, one-time task force to audit computer security is perhaps a viable temporary alternative to overcoming the lack of ADP expertise of established audit resources. In commending the HEW Task Force in chapter 1, we were basically recognizing their realization of the need, however late, of determining the extent of ADP security. Taking technicians from operating groups and giving them independent authority was an effective means of getting information for management on how well their plans were being implemented. It should be realized, however, that ad hoc groups are no replacement for concerted and continued monitoring and audit.

We share the Stanford Research Institute study's views that the attention of top management is needed and there are pressing needs for investments of money, staff, and management time to ensure the adequacy of the audit and control functions for each data processing system. (See p. 57.) The task force approach is a useful means of accomplishing a one-time assessment, but it cannot be relied upon to meet this need on a continuing basis.

CONCLUSIONS

The role of independent agency audits related to computer-based systems should be broad and multifaceted. There has already been growing acceptance that independent agency audits should include audit for economy, efficiency, and accomplishment of agencies' program objectives. Consistent with these growing responsibilities, we believe these audit organizations also should be concerned with management objectives, such as achieving adequate controls to safeguard the confidentiality and integrity of data in computer systems. At a time of increasing reliance on computers and advancing ADP technology, internal audit is a resource that is not being exploited as a means for management to meet these important responsibilities. Agency internal audit is not significantly involved in computer security because of lack of expertise, and it has not developed expertise because its involvement has not been committed.

RECOMMENDATIONS TO HEADS OF
DEPARTMENTS AND AGENCIES

We recommend that department and agency heads assign priority to developing expertise in independent internal audit organizations which would allow internal audit to assume broader responsibilities for assisting management in control of computer and data resources. Also, we recommend that heads of departments and agencies make sure that internal audit plays a continuing role in assessing computer security programs and in participating in the design of information system controls over data confidentiality and integrity.

NEED FOR AND BENEFITS OF
COMPREHENSIVE SECURITY PLANNING

The increasing use of computers by the Government and private organizations has placed computers and the systems which they serve in a highly sensitive position in today's society. The needs of the individual as well as organizations maintaining such systems require that the data be accurate and reliable. This data and these systems also must be given adequate protection from threats and hazards. Establishing secure computer systems is the way users of such systems can be assured that these requirements of confidentiality, integrity, accuracy, and reliability are being met.

In addition to our own current and previous audit reports calling attention to the need for adopting a total systems approach to developing computer systems security programs, numerous independent studies by others having professional, technical, or academic interests in these concerns have supported the concept that security planning must be comprehensive. Plans must encompass management concerns for internal control practice to achieve more than minimal levels of data integrity and protection.

The Office of Management and Budget has a special role of fiscal and policy leadership for computer systems and information management in the Federal Government. OMB has issued directives that call to the attention of heads of departments and agencies their responsibilities for programs to protect all types of sensitive data and the systems producing this information for programs under their control.

OMB's DIRECTIVES IMPLEMENTING
THE PRIVACY ACT

Specific requirements for developing computer security programs to assure confidentiality and to protect the integrity of data were issued in 1975 as part of OMB's guidelines for implementing the Privacy Act (Circular A-108 and guidelines attachment). Circular A-108 sums up these requirements for data security programs as follows.

"Each agency head shall establish and maintain procedures, consistent with the Act, OMB

guidelines, and related directives issued pursuant to this Circular, to * * * establish reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access and otherwise to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." [See 5 U.S.C. 552a(b), and (e) (10).]

The Circular delegates certain responsibilities to other central agencies. For example, the Department of Commerce (National Bureau of Standards) is made responsible for publishing standards and guidelines on computer and data security including risk management techniques. (See listing in app. II.)

In its detailed guidelines to heads of agencies, OMB has stressed the dual concerns that security programs be tailored to an agency's particular requirements and address all possible threats and hazards. It states:

"The development of appropriate administrative, technical, and physical safeguards will necessarily have to be tailored to the requirements of each system of records and other related requirements for security and confidentiality. The need to assure the integrity of and to prevent unauthorized access to systems of records will be determined not only by the requirements of this Act but also by other factors like the requirement for continuity of agency operations, the need to protect proprietary data, applicable access restrictions to protect the national security, and the need for accuracy and reliability of agency information." [Underscoring provided for emphasis.]

Although OMB had not published any directives specifically on implementing safeguard requirements related to data determined to be confidential under the Freedom of Information Act (see p. 7), the above directive should have made it

clear that all data security requirements should be considered by heads of agencies in developing their data security policies and programs.

OMB's SUPPLEMENTAL DIRECTIVE
ON RISK ASSESSMENT

In September 1975, OMB published supplemental guidance (Transmittal Memorandum No. 1 to Circular A-108) detailing to the heads of agencies new systems reporting requirements and related requirements to perform risk assessments in selecting safeguards to meet requirements of the Privacy Act of 1974.

Agencies are required to make and document studies determining the safeguards needed for specific new systems of records or for alterations of systems which create the potential for either greater or easier access. An example is the addition of a telecommunications capability which would increase the risk of unauthorized access. The directive calls for a brief description of steps taken by the agency to minimize the risk of unauthorized access to the system, including the higher or lower risk alternatives which were considered for meeting the requirements of the system.

OMB's directive is explicit in requiring use of risk assessments for determining new systems safeguards for Privacy Act systems. The requirement is implicitly required by good management practices to be applied to assessing on-going security in all present data systems as well.

OMB's NEW DIRECTIVE ESTABLISHING COMPUTER
SECURITY POLICIES AND CONTROL PROCEDURES

In September 1977, OMB circulated for comment a proposed document that would promulgate policy and detail responsibilities for the development and implementation of computer security programs by Federal departments and agencies. (The directive, Circular A-71, Transmittal Memorandum No. 1, became effective on July 27, 1978.)

The directive focused attention on the responsibilities of heads of agencies for assuring an adequate level of security for all data whether processed in-house or commercially. The scope encompassed agencies' responsibilities for protecting all personal, proprietary, or other sensitive data

not subject to separate national security regulations, as well as national security data. The OMB recognized that such areas of responsibilities may not always be clearly understood by agency management levels considering that the subject, as previously addressed, was in the limited context of OMB's guidelines for implementing the Privacy Act. 1/

The need for this directive was based on the many public concerns that have been raised in regard to risks associated with automated processing of personal and other sensitive data. The directive cites (1) problems encountered in the misuse of computer and communications technology to perpetrate crime and (2) improper payments, unnecessary purchases, or other improper actions which have resulted from inadequate administrative practices along with poorly designed computer systems.

When the draft of OMB's directive was circulated for comment, we responded to OMB's request for our views by heartily endorsing the policy draft. We noted that the proposed policy covered many of the issues and problem areas that we identified in prior reports. (See listing in app. II.)

We reminded OMB of our prior recommendations that (1) there was a need for assigning responsibilities in agencies for computer security, (2) security managers should use some form of risk analysis when deciding on what security features are cost effective, (3) controls should be established over systems using automated decision-making techniques, and (4) internal audit groups should be used to help assure management that the computer systems are under adequate control.

We observed that the policy directive addresses these problem areas. Our endorsement of the draft was given with an appreciation that the policy document would not in itself

1/These responsibilities are derived from basic housekeeping legislation now codified in 5 U.S.C. 301 authorizing heads of departments and agencies to prescribe regulations for the custody and preservation of their records, papers and property. This provision was enacted originally in 1789 by the first session of the first Congress in establishing Government agencies.

solve the agencies' problems. They must be resolved by each agency in developing its individual security programs and systems of management control. Our present report is intended to provide further impetus to heads of agencies in meeting their responsibilities.

STANFORD RESEARCH INSTITUTE STUDY

A recent Stanford Research Institute study found that

"The adequacy of internal control practices in the data processing environment has not kept pace with the expansion of data processing and the introduction of new technology and new information systems design concepts."

The Stanford Research Institute published its report in January 1977 ^{1/} on the basis of a study conducted for the Institute of Internal Auditors which shows the lagging state-of-the-art in data processing systems controls and related practices by independent internal auditors functioning in the large number of private sector firms and governmental agencies surveyed.

The report highlights important changes in recent years that have affected management's need for information to plan, evaluate, and control the operations of business and the Government and that the growth of data processing has paralleled growth in the need for management information. The study traced management's increasing dependence on data processing and, consequently, more concern about the continuing accuracy and completeness of data processing results. It concluded that management's need for new audit and control techniques have not kept pace with the growth of data processing.

Some of the report's further conclusions we share were that:

--The primary responsibility for overall internal control resides with top management, while the operational responsibility for the accuracy and

^{1/}Systems Auditability and Control Study--published in two parts: Data Processing Control Practices Report, and Data Processing Audit Practices Report. (See app. II.)

completeness of computer-based information systems should reside with users.

- Internal auditors must participate in the system development process to ensure that appropriate audit and control features are designed into new computer-based information systems.
- Verification of controls must occur both before and after installation of computer-based information systems.

The study indicated needs for the attention of top management and needs for investments of money, staff, and management time to ensure the adequacy of the audit and control functions for data processing systems.

A GOVERNMENT/INDUSTRY CONFERENCE

In March 1977, GAO representatives joined with the Institute for Computer Sciences and Technology, NBS, in organizing an invitational workshop on auditing and evaluating computer security. ^{1/} There was heavy participation by top industry computer security experts and executives responsible for this area in their companies. We observed wide acceptance, by both industry and Government representatives, for the idea that computer security programs and related management controls should be broadly defined. In this connection, computer security audit as a function of agency internal audit was recognized as a key element in a system of management controls. Internal audit and computer security audit were defined at the session as follows:

Internal audit--An independent appraisal activity within an organization for the review of operations as a service to management. The overall objective of internal auditing is to assist management in attaining its goals by furnishing information, analysis, appraisals, and recommendations pertinent to management's duties and objectives. The conferees noted that the need for effective internal auditing in the Federal agencies has been recognized by the Congress in a number of

^{1/}See "Audit and Evaluation of Computer Security" edited by Zella G. Ruthberg, NBS and Robert G. McKenzie, GAO; NBS Special Publication 500-19, issued October 1977.

laws, particularly the Budget and Accounting Procedures Act of 1950, which requires the head of each agency to establish and maintain

"* * * internal control designed to provide * * * effective control over and accountability for all funds, property, and other assets for which the agency is responsible, including appropriate internal audit."

Computer security audit--An independent evaluation to determine (1) the accuracy and reliability of the data maintained on or generated by an automated data processing system; (2) the adequacy of protection afforded the organization's assets to include hardware, software, and data from all significant anticipated threats or hazards; and (3) the operational reliability and performance assurance of the automated data processing system. We should add that the latter concept, particularly, was recognized by most managers to be in the nature of goals rather than presently achieved accomplishments in many organizations further confirming findings of both our review and the Stanford Research Institute study.

- - - -

In summary, OMB has emphasized the need for strengthening agency management directives consistent with increased awareness of these problems by organizations using computer systems or individuals served by Government programs. We strongly support OMB's position that agency computer systems security programs be developed under the broadest definition of that term.

First, to be effective, the agency's system of management controls concerned with security needs to encompass the full range of cited interests, i.e., going beyond safeguarding personal data to encompass all sensitive data; maintaining data integrity, accuracy, and reliability; and protecting the continuity of agency operations where this may be potentially affected by loss of control over sensitive data.

Secondly, when the agency's computer systems security objectives are broadly defined, the benefits from preventing

APPENDIX I

APPENDIX I

potential major losses can usually justify the costs of a reasonable level of protection.

Agencies should stress in their implementing directives the use of the abundant technical guidance that is published by the NBS, and presently available to agencies.

REFERENCE SOURCESLIST OF GAO REPORTSMultiagency or Government-wide reports
addressing selected computer security
or control issues:

1. "Challenges of Protecting Personal Information In An Expanding Federal Computer Network Environment" (LCD-76-102, Apr. 28, 1978).
2. "Proposals to Resolve Longstanding Problems In Investigations of Federal Employees" (FPCD-77-64, Dec. 16, 1977).
3. "Computer Auditing in the Executive Departments: Not Enough Is Being Done" (FGMSD-77-82, Sep. 28, 1977).
4. "Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, Mar. 31, 1977).
5. "Problems Found With Government Acquisition and Use of Computers From November 1965 to December 1976" (FGMSD-77-14, Mar. 15, 1977).
6. "Managers Need to Provide Better Protection For Federal Automated Data Processing Facilities" (FGMSD-76-40, May 10, 1976).
7. "Computer Related Crimes in Federal Programs" (FGMSD-76-27, Apr. 27, 1976).
8. "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government" (FGMSD-76-5, Apr. 23, 1976).

Reports assessing security programs
or the controls in selected
agency computer systems

1. "VA's New Computer System Has Potential to Protect Privacy of Individuals Claiming Benefits" (HRD-78-135, July 17, 1978).

2. "Procedures to Safeguard Social Security Beneficiary Records Can and Should Be Improved"--Department of HEW, Social Security Administration (HRD-78-116, June 5, 1978).
3. "Inadequacies in Data Processing Planning in the Department of Commerce" (FGMSD-78-27, May 1, 1978).
4. "Problems Persist in the Puerto Rico Food Stamp Program, The Nation's Largest" (CED-78-84, Apr. 27, 1978).
5. "Privacy Issues and Supplemental Security Income Benefits"--Department of HEW, Social Security Administration, Veterans Administration and Railroad Retirement Board (HRD-77-110, Nov. 15, 1977).
6. "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System"--Department of the Treasury, Internal Revenue Service (LCD-76-115, Jan. 17, 1977).
7. "Improved Planning--A Must Before A Department-wide Automatic Data Processing System Is Acquired For The Department of Agriculture" (LCD-76-108, June 3, 1975).

SELECTED CENTRAL AGENCY
GUIDANCE (note a)

1. "Guidelines For Automatic Data Processing Physical Security And Risk Management" (Federal Information Processing Standards Publication 31, June 1974).
2. "Computer Security Guidelines For Implementing The Privacy Act of 1974" (Federal Information Processing Standards Publication 41, May 1975).

a/Published by the Department of Commerce
(National Bureau of Standards, Institute For
Computer Science and Technology).

3. "Index of Automated System Design Requirements as Derived From the OMB Privacy Act Implementation Guidelines" August 1975 (Prepared by Task Group 15: Computer Systems Security).
4. "Security Analysis and Enhancement of Computer Operating Systems" (MBSIR 76-1041, Apr. 1976).
5. "Data Encryption Standard" (Federal Information Processing Standards Publication 46, Jan. 1977).
6. "Automatic Data Processing Risk Assessment" (NBSIR 77-1228, Mar. 1977 (Interim)).
7. "Audit and Evaluation of Computer Security" (NBS Special Publication 500-19, Oct. 1977).
8. "Performance Assurance and Data Integrity Practices" (NBS Special Publication 500-24, Jan. 1978).
9. "An Analysis of Computer Security Safeguards For Detecting and Preventing Internal Computer Misuse" (NBS Special Publication 500-25, Jan. 1978).
10. "Computer Security and the Data Encryption Standard" (NBS Special Publication 500-27, Feb. 1978).
11. "A Data Base Management Approach to Privacy Act Compliance" (NBS Special Publication 500-10, June 1977).

LIST OF OTHER REFERENCES

1. The Report of the Privacy Protection Study Commission, July 1977, "Personal Privacy in an Information Society" (Summary Report); "The Privacy Act of 1974: An Assessment" (Appendix 4). "Technology and Privacy" (Appendix 5).
2. "A Report of the Commission on Federal Paperwork, Final Summary Report," October 3, 1977; and "Confidentiality and Privacy" July 29, 1977.

3. "Systems Auditability and Control Study: Data Processing Control Practices Report"; and "Data Processing Audit Practices Report":
 - Prepared for The Institute of Internal Auditors, Orlando Florida Under a Grant From the IBM Corporation.
 - Published by Stanford Research Institute, Menlo Park, California.

LIST OF AGENCIES AND
LOCATIONS COVERED IN SURVEY

We surveyed the computer systems security programs of 10 civil agencies and visited or contacted their facilities and contractors at selected locations listed below. The agencies reviewed were the:

- Civil Service Commission.
- Customs Service, Department of the Treasury.
- Office of Education, Department of Health, Education, and Welfare.
- Energy Research and Development Administration (now part of the Department of Energy).
- Federal Energy Administration (now part of the Department of Energy).
- Bureau of the Mint, Department of the Treasury.
- National Park Service, Department of the Interior.
- Postal Service.
- Small Business Administration.
- Social Security Administration, Department of Health, Education, and Welfare.

LOCATIONS OF ACTIVITIES VISITED OR CONTACTED
DURING THE SURVEY OF COMPUTER SECURITY

<u>Activity</u>	<u>Location</u>
Administration on Aging	Washington, D.C.
Bitsmith Software, Inc.	Berkeley, Calif.
Bureau of the Mint	Washington, D.C.
Bureau of the Mint (Regional Office)	San Francisco, Calif.
City and County of San Francisco	San Francisco, Calif.
Civil Service Commission	Washington, D.C.
Civil Service Commission-- Philadelphia Region	Philadelphia, Pa.
Civil Service Commission-- Philadelphia Area Office	Philadelphia, Pa.
Customs Service	Washington, D.C.
Customs Service field activities	San Diego, Calif. San Francisco, Calif. San Francisco International Airport, Calif. San Ysidro, Calif.
Department of Health, Education, and Welfare	Washington, D.C.
Department of the Interior	Washington, D.C.
Department of the Treasury	Washington, D.C.
Energy Research and Development Administration (now part of the Department of Energy)	Germantown, Md.

APPENDIX III

APPENDIX III

<u>Activity</u>	<u>Location</u>
Energy Research and Development Administration--San Francisco Operations Office (now part of the Department of Energy)	Oakland, Calif.
Federal Energy Administration (now part of the Department of Energy)	Washington, D.C.
Federal Energy Administration-- Region III (now part of the Department of Energy)	Philadelphia, Pa.
Lawrence Berkeley Laboratory	Berkeley, Calif.
Lawrence Livermore Laboratory	Livermore, Calif.
National Institute of Drug Abuse	Rockville, Md.
National Park Service	Washington, D.C.
National Park Service-- Mid-Atlantic Regional Office	Philadelphia, Pa.
On Lok Senior Health Services	San Francisco, Calif.
Optimum Systems Incorporated	Rockville, Md.
Office of Education	Washington, D.C.
Office of Education--Region III	Philadelphia, Pa.
Postal Service	Washington, D.C.
Postal Service--Postal Data Center	San Bruno, Calif.
Social Security Administration	Baltimore, Md.
Small Business Administration	Washington, D.C.
Small Business Administration-- Philadelphia Regional Office	Bala Cynwyd, Pa.
Small Business Administration-- Philadelphia District Office	Bala Cynwyd, Pa.



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

July 27, 1978

CIRCULAR NO. A-71
Transmittal Memorandum No. 1

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Security of Federal automated information systems

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

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

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

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

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

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

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

(No. A-71)

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

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

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

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

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

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

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

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

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

(No. A-71)

responsible for assuring an adequate level of security for all agency data whether processed in-house or commercially. This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as national security data. It also includes responsibility for assuring that automated processes operate effectively and accurately. In fulfilling this responsibility each agency head shall establish policies and procedures and assign responsibility for the development, implementation, and operation of an agency computer security program. The agency's computer security program shall be consistent with all Federal policies, procedures and standards issued by the Office of Management and Budget, the General Services Administration, the Department of Commerce, and the Civil Service Commission. In consideration of problems which have been identified in relation to existing practices, each agency's computer security program shall at a minimum:

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

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

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

(No. A-71)

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

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

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

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

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

(No. A-71)

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

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

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

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

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

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

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

(No. A-71)

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

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

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

- a. Issue policies and regulations for the physical security of computer rooms in Federal buildings consistent with standards and guidelines issued by the Department of Commerce.
- b. Assure that agency procurement requests for computers, software packages, and related services include security requirements which have been certified by a responsible agency official. Delegations of procurement authority to agencies by the General Services Administration under mandatory programs, dollar threshold delegations, certification programs or other so-called blanket delegations shall include requirements for agency specifications and agency certification of security requirements. Other delegations of procurement authority shall require specific agency certification of security requirements as a part of the agency request for delegation of procurement authority.
- c. Assure that specifications for computer hardware, software, related services or the construction of computer facilities are consistent with standards and guidelines established by the Secretary of Commerce.
- d. Assure that computer equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by the General Services Administration meet the security requirements established by the user agency and are


(No. A-71)

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

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

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

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


James T. McIntyre, Jr.
Director

(No. A-71)

(941121)