DOCUMENT RESUME

07359 - [C2727830] Released

[Computer Misuse by the Sigma Corporation, a NASA Contractor]. PSAD-78-148; B-115369. September 27, 1978. Released October 12, 1978. 5 pp. + 2 enclosures (25 pp.).

Report to Sen. William Proxmire, Chairman, Senate Committee on Appropriations: HUD-Independent Agencies Subcommittee; by Robert F. Keller, Acting Comptroller General.

Issue Area: Automatic Data Processing: Guidelines for ADP Management and Control (110); Science and Technology (2000).
Contact: Procurement and Systems Acquisition Div.
Budget Function: Miscellaneous: Automatic Data Processing (1001); General Science, Space, and Technology: Supporting Space Activities (255).
Organization Concerned: National Aeronautics and Space Administration; Sigma Corp.
Congressional Relevance: Sen. William Proxmire.
Authority: Federal Computer Systems Protection Act of 1978; S. 1766 (95th Cong.). Privacy Act of 1974. OMB Circular A-71. NASA Procurement Regulation 1.605. Horne Brothers, Inc. v. Laird, 463 F.2d 1268. Myers and Myers, Inc. v. U.S. Postal Service, 527 F.2d 1252.

It was alleged that personnel from the Sigma Corporation, a National Aeronautics and Space Administration (NASA) contractor, have used NASA's main computer at Johnson Space Center to develop large-scale accounting systems and then used the systems to keep books for Sigma Corporation customers. The Federal Bureau of Investigation substantiated this allegation but declined to prosecute because the contract was completed on December 31, 1977, and NASA withheld fees due the corporation sufficient to cover the value of the unauthorized use of the computer. Most of the computer misuse occurred on other than the prime daytime shift when there was no Government surveillance. NASA decided against suspension or debarment of the corporation. Action that should be taken to prevent a recurrence of such computer misuse includes implementation of Transmittal No. 1 of Office of Management and Budget Circular A-71 which reflects policy guidance on computer security and determining the sensitivity of information and the extent to which agency resources should be invested in security and risk analysis. (HTW)

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

7830

B-115369

September 27, 1978

The Honorable William Proxmire
Chairman, Subcommittee on HUD-
Independent Agencies
Committee on Appropriations
United States Senate

Dear Mr. Chairman:

Your August 3, 1977, letter requested us to investigate an allegation that personnel from the Sigma Corporation--a National Aeronautics and Space Administration (NASA) contractor--have used NASA's main computer at Johnson Space Center to develop large-scale accounting systems and then used the systems to keep books for Sigma Corporation customers. Your letter specifically requested us to determine the facts of this allegation and to provide you any suggestions regarding steps that might be taken to prevent a recurrence of this type of alleged computer misuse.

Our initial discussions with Johnson Space Center personnel disclosed that the Federal Bureau of Investigation (FBI), at NASA's request, was also investigating the allegation. As agreed with your office, we postponed our work until the FBI completed its investigation and NASA had the opportunity to act on the findings.

The FBI has completed its investigation and its February 10, 1978, report substantiated the allegation that Sigma Corporation personnel in fact used NASA's main computer at Johnson Space Center to conduct private business. The report stated that the Assistant United States Attorney, Houston, Texas, declined to prosecute, however, because the contract between NASA and the Sigma Corporation was completed on December 31, 1977, and NASA has withheld fees due the Sigma Corporation that were sufficient to cover the value of the unauthorized use of NASA's computers.

By letter dated May 9, 1978, we requested the NASA Administrator to identify for us the specific actions that NASA took, or was planning to take, against the Sigma Corporation as a result of the FBI findings. We also asked NASA to identify any more generalized actions that were either taken or planned to prevent a recurrence of similar

instances of computer misuse at Johnson Space Center, as well as at other NASA facilities. NASA's response to our inquiry is included as enclosure I and is summarized below.

FACTS PERTAINING TO SIGMA CASE

The Sigma contract involved the use of the Space Center ADAGE CS 340 computer located in Building 13 and the Space Center UNIVAC 1110 computer located in Building 12. Sigma personnel also had direct access to the UNIVAC 1110 computer through a remote terminal in Building 13. The objective of the Sigma contract was to develop a software capability to interface the ADAGE 340 graphics computer to the UNIVAC 1110 digital computer, which is the main computer within the Space Center. The software developments involved shuttle design activities.

According to NASA, computer time was not always available to Sigma personnel on the prime daytime shift. Sigma, therefore, did much of its work on the second or third shift, during which time Government surveillance was not provided. NASA informed us that the FBI determined that the majority of the computer misuse occurred on other than the prime daytime shift, that is, when there was no Government surveillance.

Based on the FBI report and an analysis by the NASA technical monitors, it was determined that 2.82 hours of UNIVAC 1110 time was misused. This time equated to $1,213.53. In addition, three rolls of paper were used at a cost of $51.57. The total dollar value of Johnson Space Center claims against Sigma for misuse of the computer is $1,265.10.

Relative to the on-line storage time, the ADAGE CS 340 computer time, and the time which may have been used by Sigma employees on private business, there was no factual proof to cover these items and no basis on which to assess a dollar impact. At this time, NASA has held back $25,362 to cover the above claim as well as other current cost questions which are pending. The final contract audit, which is being performed by the Defense Contract Audit Agency, had not been completed at the time this report was prepared.

NASA informed us that it had considered suspension or debarment but decided against these actions. (See p. 6, enc. I.) It appears, therefore, that the parties responsible for the unauthorized use of Government facilities will go unpunished.

Regarding your concern about what actions might be taken to prevent a recurrence of this type of computer misuse, an internal NASA committee is presently reviewing existing and proposed guidelines on computer security. The committee reportedly will concentrate on implications of Transmittal No. 1, dated July 27, 1978, to Office of Management and Budget Circular A-71 (see enc. II) which reflects policy guidance on computer security provisions for the Federal Government. NASA stated that, if deemed appropriate by the committee, its guidelines will be revised to reflect specific provisions contained in Transmittal No. 1.

Also to be considered by the committee will be guidelines for carrying out risk assessments for various types of threats to the automatic data processing environment. Such analyses are important to determine the cost benefit tradeoffs of the probability of certain threats occurring versus the cost and manpower necessary to protect against them. Government surveillance guidelines for other than prime shift operations will also be discussed at some length. Data processing installation reviews with more attention to computer security provisions, as well as increased auditing, will be considered.

OUR INVOLVEMENT IN COMPUTER SECURITY PROGRAMS

Your letter requested any suggestions we might have to preclude similar incidents from occurring in the future. As you know, we have been working in the computer security area for several years and have been concerned about the need for more protection against the many types of crimes that affect computer systems. Some of the recommendations made in our prior reports were:

--That the Office of Management and Budget direct that management officials be appointed at Federal installations having computer systems and that these officials be assigned responsibility for computer security and risk management.

--That security managers, when developing and implementing security programs, use some form of risk analysis when deciding what security practices are cost effective.

--That agencies more adequately control computer systems that use automated decisionmaking techniques.

--That internal audit groups be used to help assure management that the computer systems are under adequate control.

In connection with our work in the computer security area, and at the request of the Office of Management and Budget, we reviewed a draft of Transmittal No. 1 to Circular A-71. We noted that the policy proposed in the draft covered many of the issues and problem areas that we identified in prior reports. Consequently, by letter dated October 28, 1977, we fully endorsed Transmittal No. 1. We pointed out, however, that while we concurred in this policy document, it must be recognized that it will not resolve all of the problems. There will still be problems in determining the sensitivity of information and the extent to which agency resources should be invested in security and risk analysis.

Addressing both of these issues is a necessary prerequisite to determining and specifying security requirements. We stated in our letter to the Office of Management and Budget that these issues will continue to require its attention, as well as that of the agencies being asked to implement the policy expressed in Circular A-71. NASA's response to our letter of inquiry on the Sigma case indicates that the agency plans to address these issues and, therefore, their actions are consistent with the positions we have taken regarding the steps that are needed to prevent computer fraud.

More recently, on June 22, 1978, we appeared before the Subcommittee on Criminal Laws and Procedures, Senate Committee on the Judiciary to discuss the Federal Computer Systems Protection Act of 1978 (S-1766). This bill would make it a crime to use, for fraudulent or other illegal purposes, any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce. We supported the enactment of S-1766.

As indicated in the preceding sections, we have been active in the past and plan to remain active in reviewing computer security programs. The facts involved in the Sigma case have been referred to our Financial and General Management Studies Division which has the audit responsibility in this area. That Division will fully consider these facts in scheduling its future audit work.

We trust that this information meets your needs. Since we made extensive use of NASA's written response to our letter

of inquiry concerning this matter, we did not obtain additional formal comments on the matters discussed in this report. As arranged with your office, unless you announce its contents earlier, no further distribution of this report will be made until 15 days from the date of the report. At that time, copies will be furnished to interested parties.

Sincerely yours,

T. F. Keller

ACTING Comptroller General
of the United States

Enclosures - 2

ENCLOSURE I

ENCLOSURE I

National Aeronautics and
Space Administration

Washington, D.C.
20546

Reply to Attn of: L-1

JUN 8 1978

Mr. Richard W. Gutmann
Director
Procurement and Systems
Acquisition Division
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Gutmann:

The enclosures are forwarded in response to the set of questions which were included in Mr. Day's letter of May 9, 1978, regarding the alleged misuse of a NASA computer by a contractor, Sigma Corporation.

Since NASA is a computer-intensive Agency, we are keenly aware of the potential problem areas of computer abuse or misuse and are acutely aware of the problems and needs in the overall computer security area. The draft OMB Circular A-71 on the policy and guidelines for computer security in the Federal Government has been extensively reviewed within NASA. Pending the transmittal of OMB Circular A-71 with its accompanying policy and guidelines, we will be taking some interim steps to assist our ADP managers to preclude similar incidents occurring in the future.

Sincerely,

/s/ Arnold Frutkin

Arnold W. Frutkin
Acting Associate Administrator
for External Relations

Enclosures: A/S

ENCLOSURE I

QUESTIONS AND ANSWERS PERTAINING TO COMPUTER MISUSE BY NASA CONTRACTORS

1. What actions did NASA take, either during or since the completion of the FBI investigation, to identify the underlying causes that permitted the misuse of its main computer at JSC? Please identify and elaborate on the specific problem areas to which NASA attributes the computer misuse.

The Sigma contract was performed on-site at JSC in Building 13. The contract involved the use of the JSC ADAGE CS 340 computer located in Building 13 and the JSC UNIVAC 1110 computer located in Building 12. The ADAGE computer can be used as a stand-alone computer or can be used to interface with the UNIVAC 1110 computer. In addition to these two modes, Sigma also had direct access to the UNIVAC 1110 computer through a remote terminal in Building 13. All three modes were used by other contractor and JSC employees located in Building 13. Because of the many users, computer time on prime daytime shift was not available many times and, therefore, had to be secured during second and third shifts. Sigma did much of their work on other than prime shift. Government surveillance was not provided on second or third shift. We must therefore conclude that if a contractor or its employees are disposed to misuse Government computers and Government surveillance is not present, the likelihood of the misuse is greatly increased. Even with Government surveillance, detection of "planned misuse" or "misuse in progress" is difficult. Most misuse is detected by after-the-fact audit techniques as it was in this instance.

2. The possible misuse of the NASA computer by Sigma personnel was suspected around June 1977--about 6 months before the expiration date of Sigma's contract. Sigma continued to work under the contract until it expired at the end of December 1977. Please identify the circumstances and/or consequences which prevented NASA from terminating the Sigma contract prior to the expiration date.

The objective of the Sigma activity was to develop a software capability to interface the ADAGE 340 graphics computers to the UNIVAC 1110 digital computer, which is the main computer within the JSC computing facilities. These software developments included a data management system which spans the needs of a multidisciplinary design environment; an interactive computer program to analyze weight and cost estimating relationships; and an interactive geometry module for use in preliminary Shuttle design activities. When it was discovered that the computer facilities were being misused in June 1977, Sigma had expended approximately 5 to 6 manyears' effort on these tasks (all of which would have been almost useless to JSC if they were incomplete). Therefore, it was the opinion of the JSC technical monitors that it would be to the advantage of NASA to continue the contract. The result of continuing the contract was the delivery of a completed interactive geometry module, a capability to do interactive weights and cost analyses, and the skeleton of a data base management system. Even though Sigma was allowed to continue their contract effort, JSC increased the surveillance of their work. Computer runs were regularly checked against the amount of computer time used and the files accessed during the run. No further misuse by Sigma was detected during the remaining 7 months of the contract.

3. What effect did Sigma employees working on private business while on NASA time have on the NASA/Sigma contract? Has NASA satisfied itself that the terms of the contract were met by Sigma?

We have not yet established specific proof that Sigma employees worked on private business while charging their time to the JSC contract. Part of the final audit of the contract will be to compare sign-in/out rosters in the Building 13 computer area to the employee time cards that support Sigma payrolls reimbursed by JSC. At this point, no measurable effect on the contract end products has been ascertained as a result of Sigma employees working on private business. The end products furnished by Sigma met the contract requirements.

ENCLOSURE I

4. What was the total extent of the misuse, in terms of dollars, and what has NASA done to recover the cost from Sigma?

Based on the FBI report and analysis by the NASA technical monitors, it was determined that 2.82 hours of UNIVAC 1110 time was misused. This time equated to $1,213.53. In addition, it was determined that three rolls of Gould 4800 paper was used. This equated to $51.57.

These items total $1,265.10 which is the dollar value of the JSC claims against Sigma for misuse of the computers. Relative to the on-line storage time, the ADAGE CS 340 computer time and the time which may have been used by Sigma employees on private business, there was no factual proof to cover these items and no basis upon which to assess a dollar impact. At this time, NASA has held back $25,362 which has not been paid to the contractor. These monies will be held back to cover the above claim as well as other current cost questions which are pending resolution. This final audit has not been completed at this time.

ENCLOSURE I

5. Besides recovering the cost of the misuse from Sigma, what other alternatives, such as placing Sigma on the barred bidders list, were available to NASA? Why were these alternatives rejected, i.e., what are NASA's criteria for applying each of the alternatives and in what way did the Sigma case not meet those criteria?

Debarment and suspension were considered and discussed with the JSC Legal Office. Debarment was determined inappropriate, principally because of the small sums involved and the increasing difficulties levied by the Federal courts on procuring agencies in recent years regarding the application of procedural due process in such proceedings. Reference Horne Brothers, Inc. v. Laird, 463 F2d 1268, and Myers and Myers, Inc. v. U.S. Postal Service, 527 F2d 1252. In view of our administrative ability to withhold and setoff amounts owed the Government, we felt that the resources which would be required to attempt a debarment were unwarranted. Besides, the strongest grounds for debarment (a conviction of crimes as set forth in NASA PR 1.604-2(a)) were impossible to attain because the U.S. Attorney's office had declined to prosecute.

Suspension was considered inappropriate because until the investigations were completed we did not have adequate evidence upon which to base a suspension (see NASA PR 1.605-3). Once the investigations were completed (and at about the same time the U.S. Attorney's office declined prosecution), suspension was no longer available per NASA PR 1.605-4. NASA installations will, however, be advised to contact JSC for background information prior to making a final determination of responsibility for any awards to the Sigma Corporation.

ENCLOSURE I

6. In addition to the contract in question, does NASA have any other contracts with the Sigma Corporation? If so, please identify.

JSC has had only two contracts with Sigma Corporation. The first contract (NAS 9-14520) was initiated February 10, 1975, for Engineering Design Integration (EDIN) Level I System and concluded December 27, 1976. Level I produced software to support single station, single user demand control of the design integration process. The second contract (NAS 9-15162) began December 27, 1976, and concluded December 1977. This contract was for the EDIN Level II System which provided software to support single station, single user interactive control of the design integration process. It was midway through the period of performance on the latter contract that the misuse of the computers was detected. There are no other NASA contracts with Sigma Corporation.

ENCLOSURE I

7. Has NASA let a new contract for the work previously performed by Sigma? If so, what special precautions have been taken to prevent a recurrence of the problems encountered with Sigma?

JSC has not awarded a new contract for work previously performed by Sigma. We have, however, provided the data base management system developed by Sigma to Lockheed Electronics Company, our JSC electronics lab and computer support contractor for "application" to the Space Shuttle aerodynamic base for use during the operation Flight Test Program.

8. Does NASA believe that the misuse of the JSC computer by Sigma personnel was an isolated incident or is it a problem that is evident at other NASA facilities? On what does NASA base its conclusion?

The problem of misuse or abuse of computer systems is a very difficult one. It is one that has no simple solution and is perplexing to not only NASA but the entire ADP community.

While we remain acutely aware of the possibility of similar incidents we, as well as other members of the ADP community, are faced with trying to minimize occurrence of such incidents within reasonable cost and manpower constraints. And we do feel the key must be "reasonable cost and manpower" for prevention.

Fraud, theft or embezzlement through use of a computer has occurred in the past within the business, industry, and Government environments and has received various media attention. It is a constant worry to our highly capable ADP managers. No one can say with any certainty, and even with elaborate security provisions, that it will not occur again. Even investing in extensive and elaborate security precautions will not with certainty prevent an intelligent person from "penetrating the defenses."

Indeed, it is generally agreed within the ADP community that the greatest threat for computer abuse comes from authorized users of the computer facility (as in this particular incident). Unauthorized persons, those without badges, passwords, and legitimate access to the facility are, in general, adequately controlled. However, those with authority and access to the computer in the course of their normal work represent the greatest control problem. Because of their authorization to use the computer in the normal work and their sophisticated knowledge, they are also the most difficult to detect in unauthorized activities.

While we can consider this an isolated incident and not a significant problem at our computing facilities, we also recognize that the potential exists for this type of incident occurring again. We would be less than candid or realistic to state otherwise. However, we intend to stay alert to this type of incident and take those precautions which appear reasonable in terms of overall cost-effectiveness. Certainly those activities in which the data being handled is of a sensitive or intrinsically high-risk nature will continue to be subject to greater surveillance and procedural precaution.

ENCLOSURE I

9. Has NASA alerted all its facilities regarding the problem of computer misuse and have instructions been issued on how to tighten the security over the use of NASA's computers? If so, please summarize and provide copies of those instructions.

Although no formal comprehensive instructions have been issued to date, NASA field installations are continually kept apprised of developments in the area of computer misuse. Such communication has been in the form of various correspondence and presentations at our annual or special meetings of the computer community. Also, the draft policy guidance contained in the proposed Transmittal Memorandum No. 1 to OMB Circular A-71 was disseminated and discussed several months ago. (See GAO note.)

At the present time, a committee is reviewing existing and proposed guidelines on computer security. This committee will concentrate on implications of the draft A-71 Transmittal Memorandum, reflecting policy guidance on computer security provisions for the Federal Government. If appropriate, NASA guidelines will be revised to reflect specific provisions as proposed in this document. Also to be considered by the committee will be guidelines for carrying out risk assessments for various types of threats to the ADP environment. Such analyses are important to determine the cost benefit tradeoffs of the probability of certain threats occurring versus the cost and manpower necessary to protect against them. Government surveillance guidelines for other than prime shift operations will also be discussed at some length. DPI reviews with more attention to computer security provisions, as well as increased auditing, will be considered.

The implementation of procedures and safeguard plans for the Privacy Act of 1974 provisions involving "personal" data at our field installations afforded recent opportunity to assess the security of other data as well as general physical security practices. During the course of security reviews involving personal data there also began a conscious effort to review the entire process of security for the overall ADP environment.

It has been recognized that highly detailed guidelines on computer security cannot be issued to our field installations from the Headquarters due to the wide and diverse locations, the differing types of equipment, the physical layouts of the computing facilities, the types and amount

GAO note: Transmittal No. 1 to OMB Circular A-71 was issued on July 27, 1978.

ENCLOSURE I

of workloads being run on the computers, etc. However, broad and comprehensive guidelines are being incorporated in the NASA ADP management handbook to cover security provisions. These Headquarters guidelines will be flexible so that the field installation can incorporate and modify their security controls to fit the local conditions while providing maximum protection.

10. Are there any other instances of computer fraud that have been discovered within the past 2 years at NASA facilities? If so, please provide the details and disposition of each case.

Over the past 2 years, NASA has experienced one additional serious instance of computer misuse. This matter was brought to light during a routine inspection of computer directories and promptly reported, thus enabling a timely investigation. Investigation revealed that a NASA contract employee and a former contract employee had formed an electronics firm and misused a NASA computer by developing and storing the firm's marketing plans, technical manuals, plus other writings and computer architecture details--all of which were unrelated to Government business. The investigation also uncovered the fact that both subjects were involved in the theft of Government property (hardware), over $5,000 of which was recovered. Based on commercial computer costs for the same services, NASA estimates the total amount of misuse to be $1,924. Both subjects were indicted by the Federal Grand Jury for grand theft, conspiracy, and theft of computer time and storage. On April 14, 1978, both subjects appeared in Federal Court and as a result of plea bargaining, one pled guilty to petty theft and the other to a felony, grand theft of computer time and storage. They are to appear in Federal Court on June 9, 1978, for sentencing. (See GAO note.)

GAO note: One subject was sentenced to 2 years imprisonment which was suspended. He was placed on 1 year probation.

The other subject was sentenced to 3 years imprisonment which was suspended. He was placed on probation for 4 years, fined $1,000 and ordered to make restitution to NASA for $2,000.

11. Are there other instances currently under investigation? Please provide the details and status of each case.

There are no other instances under investigation at this time.

ENCLOSURE II

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

ENCLOSURE II

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

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

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

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

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

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

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

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

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

responsible for assuring an adequate level of security for all agency data whether processed in-house or commercially. This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as national security data. It also includes responsibility for assuring that automated processes operate effectively and accurately. In fulfilling this responsibility each agency head snall 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,

ENCLOSURE II

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

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

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

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

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

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

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

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

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

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

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

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

ENCLOSURE II

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

ENCLOSURE II

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.

James T. McIntyre, Jr.
Director

(No. A-71)

ENCLOSURE II

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

MARCH 6, 1965

CIRCULAR No. A-71

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Responsibilities for the administration and management of automatic data processing activities

1. Purpose. This Circular identifies certain responsibilities of executive agencies for the administration and management of automatic data processing (ADP) activities, and is intended to provide for maximum cooperation and coordination between and among the staff and operating agencies of the executive branch.

2. Scope. The ADP equipment affected by this Circular is that equipment identified in paragraph 2 of Bureau of the Budget Circular No. A-54, Policies on the selection and acquisition of automatic data processing (ADP) equipment, October 14, 1961.

3. Responsibilities of the Bureau of the Budget. The Bureau of the Budget will provide overall leadership and coordination of executive branch-wide activities pertaining to the management of automatic data processing equipment and related resources and will develop programs and issue instructions for achieving increased cost effectiveness through improved practices and techniques for the selection, acquisition and utilization of automatic data processing equipment and resources. In this connection, the Bureau of the Budget will:

a. Provide policies and criteria, procedures, regulations, information, technical advice and assistance to executive agencies.

b. Evaluate, through the review of agency programs and budgets and through other means, the effectiveness of executive agencies and the executive branch as a whole in managing automatic data processing equipment and resources.

c. Foster adequate Federal Government support of programs for developing voluntary commercial standards for automatic data processing equipment and techniques, arrange for the approval and promulgation of voluntary commercial standards when it is in the best interests of the Government to do so, and arrange for the development, approval and promulgation of Federal standards for automatic data processing equipment and techniques on an interim basis, or permanent basis, when voluntary commercial standards are not available or usable.

ENCLOSURE II

d. Support the development and promulgation of standard data elements and codes in Government systems, when such data elements and codes are in common use in some or all executive agencies.

e. Encourage the use of advanced techniques in the design of data systems and support research in advanced system design through demonstration projects.

f. Advocate intra-agency and interagency integration of systems.

g. Sponsor the development of a system which provides to line and staff officials at all levels of Government the information needed for effective management of automatic data processing equipment and related resources.

4. Responsibilities of the General Services Administration. The General Services Administration is responsible for aiding in the achievement of increased cost effectiveness in the selection, acquisition and utilization of automatic data processing equipment and appropriate related resources and will perform the following functions:

a. In connection with the selection of automatic data processing equipment, provide to executive agencies, on request, comparative information on the characteristics and performance capabilities of equipment and on the contractual performance of the firms that supply equipment and programing aids to the Government.

b. In connection with the acquisition of automatic data processing equipment (1) provide Federal Schedules of Supply for renting, purchasing and maintaining automatic data processing equipment, for use by executive agencies each fiscal year, (2) take such steps as may be feasible and necessary to insure to the extent practicable, that the Federal Schedules of Supply for ADP equipment each year will be available for use on the first day of that year, and (3) through continuous study and negotiation, seek improvements in the terms, conditions, and prices stated in Federal Schedules of Supply for automatic data processing equipment and services.

c. In connection with the utilization of automatic data processing equipment (1) develop and publish guidelines and criteria governing the replacement of equipment to avoid usage of such equipment beyond the point of economic advantage, (2) provide overall coordination and leadership of the executive branch in fostering the effective utilization of excess and disposal of surplus, automatic data processing equipment, including rented, leased or owned equipment, and promulgate such regulations as may be needed to insure effective Government-wide screening and utilization of excess ADP

equipment; and, further, to plan and undertake appropriate measures for coping with emerging problems associated with the management of excess and surplus automatic data processing equipment, (3) prepare Government-wide inventory reports and other statistical information pertaining to ADP equipment utilization, based upon reports submitted in accordance with applicable Bureau of the Budget circulars; and, further, to cooperate in the continuous refinement and improvement of management information systems relating to automatic data processing activities, (4) exercise leadership for the executive branch in the development and operation of arrangements which are designed to promote the sharing and joint utilization of automatic data processing equipment time and services within and among the executive agencies, and obtain such information on sharing practices as is necessary to evaluate the sharing program on a Government-wide and regional basis, including acquisition of equipment in connection with joint utilization programs, and (5) provide policies, guidelines and evaluation criteria for use by executive agencies in the maintenance of automatic data processing equipment.

d. In connection with the standardization of automatic data processing equipment and techniques, (1) promulgate standard purchase specifications based upon ADP standards which have been approved for adoption by the Federal Government, and (2) support programs for the development of voluntary commercial or Federal standards as they pertain to automatic data processing equipment and techniques and coordinate these activities with other executive agencies similarly involved.

e. In connection with automatic data processing equipment used with data communications systems, insure that planning for the Federal Telecommunications System embraces consideration of the rising need for data communication facilities which provide for high-speed data transmission between computer-based systems.

5. Responsibilities of the Department of Commerce. The Department of Commerce is responsible for aiding in the achievement of increased cost effectiveness in the selection, acquisition and utilization of automatic data processing equipment, and in this connection will perform the following functions:

a. Provide advisory and consultative services to executive agencies on the methods for developing information systems based on the use of computers and the programing and languages thereof.

b. Undertake research on computer sciences and techniques, including system design, oriented primarily toward Government applications.

ENCLOSURE II

c. Provide day-to-day guidance and monitorship of an executive branch program for supporting the development, measurement and testing of voluntary commercial standards for automatic data processing equipment, techniques and computer languages.

d. Improve compatibility in automatic data processing equipment procured by the Federal Government by recommending uniform Federal standards for automatic data processing equipment, techniques and computer languages.

6. Responsibilities of the Civil Service Commission. The Civil Service Commission is responsible for providing executive branch-wide leadership and assistance in the personnel management and manpower aspects of automatic data processing. In this connection, the Commission will foster programs designed to:

a. Staff automatic data processing activities effectively by, among other things, (1) formulating position classification and qualification standards, (2) developing necessary special recruiting techniques, (3) devising improved testing and selection devices, and (4) stimulating and coordinating necessary training.

b. Educate executives and other key personnel to achieve greater effectiveness in ADP management.

c. Anticipate and minimize, to the greatest practicable extent, any adverse effects of automatic data processing upon the people involved.

d. Provide a medium within the executive branch to focus and coordinate preparation for the future personnel management and manpower effects and requirements of automatic data processing.

7. Responsibilities of the heads of executive agencies. The heads of all executive departments and establishments are responsible for the administration and management of their automatic data processing activities including:

a. Agency-wide planning, coordination and control of equipment utilization.

b. Determination and use of those equipment applications that offer the greatest return in terms of increased effectiveness in mission accomplishment and higher productivity.

c. Development of data systems that employ the use of the most advanced design techniques.

ENCLOSURE II

d. Merger or integration of data systems irrespective of intra-agency or interagency organizational lines, when cost effectiveness in equipment utilization, data systems management, or program accomplishment can be increased.

e. Determination of automatic data processing equipment requirements.

f. Sharing equipment time and services within the agency, and with other agencies through support of the Government-wide program for sharing exchanges; cooperation in the establishment of service centers and other interagency joint use arrangements.

g. Consideration of the potential impact of the introduction of ADP equipment on the agency work force and taking such steps as are necessary to alleviate adverse effects to the greatest extent practicable.

h. Participation in Government-wide studies and programs for improving the administration and management of automatic data processing activities in the executive branch.

8. Effective date. The provisions of this Circular are effective immediately.

KERMIT GORDON
Director

(No. A-[illegible])