DCCUMENT SESUME

06218 - [B1586605] ~~(Restricted)~~ RELEASED

Procedures to Safequard Social Security Beneficiary Records Can and Should Be Improved. HRD-78-116; B-164031(4). June 5, 1978. 28 pp. + 4 appendices (13 pp.).

Report to Rep. Charles Rose; Rep. John E. Moss; by Elmer B. Staats, Comptroller General.

Issue Area: Income Security Programs: Program Monitoring and Administration (1303).
Contact: Human Resources Div.
Budget Function: Income Security: Public Assistance and Other Income Supplements (604); Income Security: General Retirement and Disability Insurance (601).
Organization Concerned: Department of Health, Education, and Welfare; Social Security Administration.
Congressional Relevance: Rep. Charles Rose; Rep. John E. Moss.
Authority: Freedom of Information Act.

The Social Security Administration (SSA) is responsible for making correct and timely payments to individuals entitled to benefits under social insurance and welfare programs and for providing support functions for the medicare program. These programs generate millions of records on workers and beneficiaries that are maintained in automated data banks and files. Findings/Conclusions: Personal files within the data system contain valuable private information that is necessary to support present and future Social Security benefits. SSA uses a vast computerized telecommunications network to process its workload and to handle inquiries from the public. The telecommunications system contained certain security weaknesses: the ability to create as well as query beneficiary files from most terminals, failure to use audit trail features within the system, failure to always lock terminals during nonworking hours, and unlimited unrestricted access to terminals. Files containing personal data on beneficiaries such as earnings records, financial status, and medical evaluations were not being properly safeguarded from potential loss, destruction, abuse, or misuse. SSA had not issued guidelines or criteria for establishing physical security measures at field offices and had not determined if adequate security was provided in the handling of information by States in administering welfare programs and by insurance companies in administering medicare. Recommendations: The Secretary of Health, Education, and Welfare should direct the Commissioner of SSA to correct weaknesses in the telecommunications network and continue to pursue an active security program to assure the Congress, the public, and beneficiaries that records are properly safeguarded. In this effort, the Secretary should conduct a risk analysis to determine how best to correct physical security weaknesses, including measures which will achieve a balance between good service to beneficiaries and good security. (HTW)

6605

REPORT BY THE

Comptroller General

OF THE UNITED STATES

Procedures To Safeguard Social Security Beneficiary Records Can And Should Be Improved

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.

HRD-78-116
JUNE 5, 1978

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

B-164031(4)

The Honorable Charles Rose
The Honorable John E. Moss
House of Representatives

Your March 30, 1976, letter requested an investigation of the Social Security Data Acquisition and Response System. During this review, we met with your representative and agreed to expand the review to determine if Social Security procedures were adequate to prevent misuse of beneficiary records (both automated records and documents supporting beneficiary claims).

This report contains our findings on security procedures used to protect beneficiary records at Social Security offices, State disability determination offices, and private insurance companies.

We identified security and management problems which could lead to potential loss, destruction, abuse or misuse of both the automated and hard copy records maintained by Social Security. Since the start of this review, Social Security has taken action to improve its security procedures.

At your request, we did not take the additional time to obtain written comments from the Department of Health, Education, and Welfare. The matters covered in this report, however, were discussed with Social Security officials, and their comments are incorporated where appropriate.

As arranged with your office, unless either of you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of the report. At that time, we will send copies to the Department of Health, Education, and Welfare and other interested parties, and make copies available to others upon request.

Comptroller General
of the United States

REPORT OF THE
COMPTROLLER GENERAL
OF THE UNITED STATES

PROCEDURES TO SAFEGUARD SOCIAL SECURITY BENEFICIARY RECORDS CAN AND SHOULD BE IMPROVED

D I G E S T

The Social Security Administration, a constituent agency of the Department of Health, Education, and Welfare

--is responsible for making correct and timely payments to individuals entitled to benefits under the Nation's social insurance and welfare programs and

--provides support functions, including data processing services, for the Medicare program.

It relies in part on contractual services provided by States and insurance companies to carry out its responsibilities related to these programs.

These programs generate millions of records on workers and beneficiaries that are maintained in automated data banks and files. The records constitute a valuable national resource that must be safeguarded against alteration, destruction, abuse, or misuse. Personal files within the data system contain valuable private information on workers and beneficiaries that is necessary to support present and future Social Security benefits. To process its workload and handle inquiries from the public, Social Security uses a vast computerized telecommunications network. (See ch. 1.)

GAO found the following types of telecommunications system design and management problems which lead to security weaknesses in safeguarding automated beneficiary records. (See ch. 2.)

--Ability to create as well as query beneficiary files from most terminals.

--Failure to use audit trail features within the system.

--Failure to always lock terminals during nonworking hours.

--Unlimited and unrestricted access to terminals.

Social Security field offices, private insurance companies, and State disability determination services need to better protect documents in files supporting beneficiary claims.

There are thousands of these files in most offices, and they contain personal data on beneficiaries such as earnings records, financial status, and medical evaluations. They are not being properly safeguarded from potential loss, destruction, abuse, or misuse. (See ch. 3.)

Social Security had not issued any guidelines or criteria for establishing overall physical security measures at its field offices. Moreover, few guidelines have been issued on safeguarding the documents in the files being processed within these offices.

Social Security submits beneficiary information to (1) States for their use in administering welfare programs and (2) insurance companies for their use in administering Medicare. The organizations, in turn, distribute the information to their local offices. Social Security has not determined if adequate security is provided in these situations. (See ch. 3.)

The Commissioner of Social Security has identified security as a major priority. In February 1977, a system security staff was permanently established. Since that time, this group has released several publications and taken actions on security matters. It has (1) distributed several training pamphlets and a system security handbook, (2) conducted

security reviews of 200 field offices and certain central office components, and (3) completed a study of computer-related crime vulnerability of one major program. It plans to conduct security reviews of all field offices and complete studies of other major programs during 1978.

The Secretary of Health, Education, and Welfare should immediately direct the Commissioner of Social Security to correct weaknesses in the telecommunications network identified in this report. He should also continue to pursue an active and aggressive security program to assure the Congress, the public, and beneficiaries that records are properly safeguarded against abuse, misuse, destruction, or alteration. In this effort, the Secretary should conduct a risk analysis to determine how best to correct the physical security weaknesses identified in this report and determine whether other security weaknesses exist. The effort should include security measures in terms of efficient and effective services to beneficiaries; a balance between good service and good security should be weighed. (See ch. 4.)

Contents

ABBREVIATIONS

ARS	Advanced Records System
GAO	General Accounting Office
GSA	General Services Administration
HEW	Department of Health, Education, and Welfare
SSA	Social Security Administration
SSADARS	Social Security Administration Data Acquisition and Response System
SSI	Supplemental Security Income

CHAPTER 1

INTRODUCTION

On March 30, 1976, Congressmen John E. Moss and Charles Rose requested that we review the Social Security Administration Data Acquisition and Response System (SSADARS) telecommunications network. They requested that we answer certain specific questions concerning equipment utilization and design, expansion plans, and privacy of information in the SSADARS network.

In January 1977, after visiting the Social Security Administration (SSA) headquarters and several field offices, we advised the representative for both Congressmen that

--SSADARS was only a part of the automated telecommunications network and

--significant security problems existed (1) with other segments of this network and (2) also with physical security measures used by many field locations to safeguard assets and beneficiary data.

It was agreed that the review should be changed to evaluate SSA's physical security procedures as well as security features within the automated system, primarily the Advanced Records System (ARS) and SSADARS, rather than answer specific questions included in the original request. It was further agreed that these evaluations should be made at many SSA field offices, private insurance companies, and State disability determination offices under contract with the Department of Health, Education, and Welfare (HEW).

SSA is a constituent agency of HEW and is responsible for making correct and timely payments to individuals entitled to benefits under programs authorized by titles II and XVI of the Social Security Act, as amended. These programs include

--retirement and disability insurance programs designed to provide cash benefits to replace, in part, earnings that are lost to individuals and families when earnings stop or are reduced because the worker retires, dies, or becomes disabled and

--the Supplemental Security Income programs designed to provide cash benefits to the needy, aged, blind, and disabled.

SSA is also responsible for administering the Aid to Families with Dependent Children program, which provides Federal funds enabling States to furnish financial assistance, rehabilitation, and other services to needy families with dependent children.

The Health Care Financing Administration, another constituent agency of HEW, is responsible for making payments on behalf of individuals entitled to benefits under the Medicare program, authorized by title XVIII of the Social Security Act, as amended. Medicare provides partial protection against the cost of health care for the aged and severely disabled. SSA provides support functions, including data processing services for the Medicare program.

As of September 1977, about 80,000 full-time permanent personnel were employed at Social Security headquarters in Baltimore, Maryland; 6 program service centers; 10 regional offices; and over 1,300 district and branch offices nationwide to administer these programs. HEW also relies on contractual services provided by many State agencies (making disability determinations) and insurance companies (administering Medicare programs as intermediaries and carriers) to carry out its responsibilities related to these programs.

These programs generate a huge recordkeeping workload. In fiscal year 1977, more than 33 million beneficiaries received about $103 billion. Most of this workload is handled on electronic data processing systems located at agency headquarters. These data processing operations 1/ include estabishing new Social Security numbers, computing program benefits, maintaining program beneficiary rolls, maintaining and updating individual lifetime earnings records for over 170 million workers, and providing data processing support for the health insurance process.

1/Does not include operations supporting the Aid to Families with Dependent Children program, which may eventually be performed on these systems.

The data banks maintained by SSA constitute a large national resource that must be safeguarded against alteration, destruction, abuse, or misuse. Timely and correct payments to beneficiaries might be impossible if this resource were altered or destroyed. Moreover, many other Government agencies, as well as industry, rely on information generated from these automated data banks in managing their operations. In addition to the composite value of these large data banks, the personal files within the system are valuable to the workers and their families in that they contain private personal information gathered to support present and future payments made under Social Security and Medicare programs.

In fiscal year 1977, SSA processed about 149 million initial claims and 539 million post-entitlement and record maintenance actions. To process this workload and be responsive to many personal inquiries from beneficiaries, SSA operates a vast compyterized telecommunications system.

SSA TELECOMMUNICATIONS EQUIPMENT DESIGN AND OPERATION

SSA uses basically three methods of communicating between the data bank at its headquarters in Baltimore and its field offices, private insurance companies, and State agencies located throughout the country:

--ARS.

--SSADARS.

--Programable magnetic tape terminals (using dedicated leased communications lines).

As mentioned above, our review concentrated on ARS and SSADARS.

Both ARS and SSADARS provide on-line data retrieval and file update capabilities to SSA field offices, private insurance companies, and State agencies.

ARS

ARS is a telecommunications system, maintained by the General Services Administration (GSA) for use by many civil Federal agencies. SSA started using this system on May 1, 1966. As of November 1, 1977, 192 of SSA's

1,454 ARS teletype terminals 1/ were located at State agencies and private insurance companies operating as contractors. The remaining terminals are located at SSA offices throughout the country.

SSADARS

SSADARS is a nationwide, high-speed, data communication system developed for use by SSA. This system was implemented during January 1974 and was designed to (1) augment ARS teletype terminals in the field and (2) relieve the ever-increasing data processing workload. The start and stop point for most SSADARS transactions are the keystations located at SSA field offices, State agencies, or private insurance companies. An office can have from 2 to 16 or more key stations 1/ depending on its size and workload. As of November 1, 1977, 33 of the 2,315 terminals in the network were located at State agencies and private insurance companies; the remaining units were located at SSA offices.

SSA has six program service centers, equipped with computers and other devices which serve as communication links between the offices in the field and the central computer facility. Each center has a minicomputer, a terminal identical to the field office terminals, and technical control equipment.

SCOPE OF REVIEW

Our review was performed at: (1) SSA headquarters; (2) 22 SSA field offices; (3) 1 program center; (4) 8 State disability determination offices; and (5) 4 private insurance companies. The installations were located in Alabama, California, Connecticut, Florida, Hawaii, Illinois, Kansas, Maine, Maryland, Massachusetts, New Hampshire, Nevada, Pennsylvania, and Vermont. They encompassed 6 of 10 SSA regions.

We interviewed officials at each of these locations and examined records concerning security matters. We did not attempt to identify all of the multitude of security problems in various SSA systems. However, we evaluated selected technical, administrative, and physical safeguards in the communications network.

1/ ARS teletype terminals and SSADARS keystations, as defined by SSA, are referred to as terminals throughout the remainder of this report.

CHAPTER 2

LIMITED SAFEGUARDS ARE PROVIDED TO PROTECT AUTOMATED BENEFICIARY RECORDS

Computerized files are maintained on all claimants who have applied for or are receiving benefits from SSA programs and Medicare. Such files can be changed or accessed for information through use of SSADARS or ARS. Eligibility information from the computerized claimant files is duplicated on microfiche, and copies are distributed to the field offices of jurisdiction every 3 months. The security of the microfiche files is discussed in chapter 3.

We found the following types of system design and management problems which lead to security weaknesses in safeguarding automated beneficiary records:

--Ability to create as well as query beneficiary files from most terminals.

--Failure to use audit trail 1/ features within the system.

--Failure to always lock terminals during nonworking hours.

--Unlimited and unrestricted access to terminals.

ABILITY TO CREATE AS WELL AS QUERY BENEFICIARY FILES FROM MOST TERMINALS

The automated telecommunications system was designed to (1) access the huge data base of information on beneficiaries and (2) assist field offices in initiating claims, obtaining information, and making changes to beneficiary files. During the design phase, major emphasis was placed on providing service to the beneficiary. Security over information within the system was not a prime design factor. For example, the system does not

---

1/ A means for identifying action taken in processing data so that it can be traced back to the individual originating the transaction.

restrict employees to the performance of transactions which are related to their specific duties and responsibilities.

Over 3,700 terminals are located on the SSA telecommunication network, including about 180 in State agencies, and 40 in private insurance companies. The terminals in SSA field offices and State agencies have a full capability to create, access, and change beneficiary files. It was not until late 1975 that SSA began restricting the capabilities of terminals in private insurance companies to assessing and making changes only to those records related to the Medicare program.

We visited four private insurance company offices during our review to test the validity of access restrictions. Two of these offices were using SSADARS, and the remaining two offices were using ARS. Through use of this equipment, we attempted to access complete beneficiary files. All of our attempts were blocked except for access to the portion of beneficiary records needed to process Medicare claims.

As a result of these tests, we directed our effort to evaluating security features on the terminals located in SSA field offices and State agencies. A user at any of these terminals can access and make changes to the millions of active beneficiary records stored within the national data bank.

For example, State agencies which are only responsible for making medical determinations for title II and Supplemental Security Income (SSI) disability claims also have the capability to create new SSI claims and enter changes to existing SSI records. Likewise, teleservice centers which handle many of the telephone contacts with SSA recipients only have authority to make changes to existing records, which do not affect payment amounts, but have the capability to create initial claims as well as enter changes.

Additionally, State agencies and SSA field offices have access to all beneficiary records for the programs they service. These records contain information as shown in appendix I.

Most field offices have several terminals available for use by employees. Some of these terminals are located in restricted areas, and others are located in unrestricted areas throughout the installations. Because there are terminals in open areas, local managers have attempted to designate specific terminals for data input functions and

have left others open for use by anyone in the office. This approach does not preclude the potential for misuse or abuse of the system or beneficiary data by employees, systems maintenance representatives, or other potential wrongdoers.

FAILURE TO USE AUDIT TRAIL FEATURES WITHIN THE SYSTEM

One significant element of internal control within computerized systems is an audit trail whereby each transaction can be associated with offices and users. The automated system used by SSA, State agencies, and insurance companies has been designed to provide such an audit trail for identifying the office and each person within an office that uses the system.

The office identifier is required on each transaction processed and is used as an address for the system to respond to the originating office. Thus, an audit trail exists for tracing transactions from the central complex to the originating office. Identification of personal users, however, was left as an optional feature within the system design, and such identification is not required to use the system. Several field offices included in our review frequently use this feature to identify a division or work station so that printed output can be routed to its proper location. We observed that most offices do not require personal identifiers. Thus, the capability to relate all transactions to specific users of the system is not being used. To help prevent fraudulent claims or changes to existing records, personal identifiers, such as an employee's initials, could also be required on documents used to input transactions. Initials could be required for the employees who (1) interview the claimant, (2) prepare the input documents, and (3) review the input documents and supporting documentation. Additional automated identifiers could be used for all transactions entered over terminals (such as a user identification as discussed on pp. 12 and 13).

The need for a good audit trail from the system to the individual user becomes even more important within the SSA system because of (1) the magnitude of personal information being processed on the system, (2) the ability to query files from anywhere in the country, and (3) the existence of a procedure used by SSA called "Alternate Mode of Operation."

Alternate mode was built into the system to provide backup when equipment failures occur. Additionally, users can input information from one SSA office and make the system believe that it came from another. Moreover, any data messages (query, creation of initial claims, administrative messages, etc.) can be initiated from one office, and the response can be received at another anywhere in the country. This is useful if an SSA office's printer is not working; the office can query the data bank and have the message printed out at another nearby SSA office. In the absence of audit trails and personal identifiers, it is difficult to identify individuals that are abusing their access to beneficiary information; as a result, abuses can occur. For example, as reported in the press, a private company built a flourishing business by gaining unauthorized access to Federal medical records and selling the information to many of the Nation's largest insurance companies. Data supporting this personal information was obtained from many sources, including SSA employees. SSA officials responded to this problem by stating that they had no indication that information from agency files had been obtained by the company.

Although personal identifiers and audit trails, in themselves, will not eliminate abuses by individuals, they will assist as a deterrent when combined with other controls to restrict unauthorized access to beneficiary information.

FAILURES TO LOCK TERMINALS DURING NONWORKING HOURS

SSA field offices and State agencies transmit information to and obtain information from headquarters data banks located in Baltimore by using ARS and SSADARS terminals. Offices using SSADARS terminals communicate all transactions with Baltimore through equipment located in SSA program centers. However, offices using ARS terminals route queries through SSA program centers and input information, such as initial claims and changes to existing records, through GSA facilities.

It was not until November 1975 that a procedure was established for offices using terminals transmitting information through the SSA program centers to lock the terminal equipment to prevent unauthorized use. This procedure does not apply to the ARS transmissions routed through the GSA facility.

The lock/unlock procedure requires that each office establish a password which is transmitted to Baltimore to lock the terminals at the end of the working day. Once headquarters has accepted a message to lock the system from a field office, no additional beneficiary information can be transmitted on the terminals until they are unlocked using the same password that was used to lock the system.

Except for general physical security measures--door locks, guard service, burglar alarms, etc.,--the lock/unlock procedure is the only means available within the existing SSA system to safeguard it against unauthorized use during nonworking hours. No similar procedure has been established for ARS transmissions routed through GSA facilities. Consequently, they remain open for use at all times.

In offices where terminals can be locked, we were told by field office officials that there are many instances when they cannot lock their terminals because of equipment failures. Therefore, their terminals remained open and could be used by unauthorized persons during nonworking hours.

The password used to lock/unlock the terminals can be considered as the key to the SSA national data bank. The design for this feature allows for changing passwords each time that the terminals have been locked and unlocked. We found a wide range of time intervals used by field offices for changing passwords--daily, weekly, monthly, quarterly, semiannually, annually, etc. (See app. II.) Moreover, 7 of the 36 installations included in our review had never changed the password since implementation of the lock/unlock procedure, and two installations only change the password when there is a turnover of employees who know the password. SSA reviewed the use of the lock/unlock procedures and found that compliance had been lax. On March 30, 1977, SSA issued instructions to the field offices to strengthen the use of this procedure.

However, in July 1977, we visited several offices and found that they were still not changing passwords routinely. Numerous data transmission personnel knew both the password being used and the appropriate lock and unlock procedures.

The design for establishing system passwords may contain letters, numerals, or any combination of the two. We found that field offices use different methods for establishing the password for their terminals. Two examples are (1) numeric expressions of the month and day of the change and (2) selected words.

Once established, the method may be used thereafter consistently. Using the same method for changing passwords can subject an automated system to greater potential of compromise, especially when a system is available for use by many people within an organization. Over a period of time, the basis for creating a password can be deciphered when continually used. Authorities on security matters have stated that passwords should be changed frequently. In our opinion, this should be accomplished by changing the password at least monthly.

UNLIMITED AND UNRESTRICTED ACCESS TO TERMINALS

As previously discussed, most terminals in the SSA system (located in district/branch offices and teleservice centers) have a full capability to create, access, and change beneficiary files. We found that local management determines where terminals are placed and what functions will be performed on the terminals. In some offices, employees had been instructed to use certain terminals located throughout the office for querying beneficiary records, and other terminals for input only. Since local managers rely on observation by supervisors or employee challenges to enforce this procedure, it seems to us (and office personnel agree), that this does not provide adequate control for preventing unauthorized use of the terminals.

Some offices have dispersed terminals throughout the office and reception areas in order to better serve the public. However, other offices have placed their terminals in a separate room. In cases where the terminals were in one room, some local management officials said they could exercise better control over use of the equipment. However, even in these offices, access to the terminal room was not restricted to selected, designated individuals such as data transmission personnel and their immediate supervisors, the manager, and the security officer. The placement of terminals throughout an office leaves the automated systems open for possible use by those who have access to the office.

Some offices have obtained greater control over their terminals' usage by locating their printer in a secure terminal room. This could allow data transmission personnel to continually monitor all printed output as well as separate it for the appropriate employee to pickup.

Without the necessary manuals and forms to decipher information obtained from the system, or to query or input changes to existing records, it would be difficult for

individuals to use the terminals. SSA has developed many forms showing formats required for entering data into the system. These forms have been made available to most all employees within the various field offices. Also, manuals showing how to use the system and how to interpret data received from the system, for the most part, are left in open areas and not safeguarded during nonworking hours. Moreover, agency guidelines provide that these manuals can be reviewed by the general public, upon request, in accordance with the Freedom of Information Act, at SSA field offices. Many field offices have also posted summaries of these interpretative guides on walls by the terminals to assist operators when using the system to query automated beneficiary records.

SSA employees have abused the capabilities of the automated system. For example, as reported in the press, one employee was selling Social Security cards to illegal aliens and others who desired a new identity. Because this employee had access to the computer system and knew how to use it, he would summon up the names and Social Security numbers of people who had died. Then he would type those names and numbers on Social Security cards--stolen from the office--and sell them in the underground market.

In another instance, (reported in the press), an SSA district office employee redirected Social Security payments to himself by inputting changes of addresses rather than inputting a stop payment because of a beneficiary's death. This employee netted about $20,000 in fraudulent claims before being apprehended.

Maintenance contractors use the terminals when correcting or checking out mechanical problems in the network. These individuals are not required to use personal identifiers, and local office management does not always supervise their activities while using the automated system. Therefore, it is possible that such individuals could obtain automated records or input invalid transactions.

In addition to maintaining beneficiary records, the SSA system can be used to trigger cash payment to certain beneficiaries. When certain cases are determined critical by field office employees, they can immediately initiate payment action by entering appropriate data into the automated system. This program was initiated in February 1976. As of November 1977, there have been about 190,000 cases involving about $219 million. Such transactions require adequate control to prevent employees or others from abusing the system.

PLANNED EXPANSION OF THE AUTOMATED TELECOMMUNICATIONS SYSTEM

Another consideration regarding SSA controls over the system is that SSA plans to eliminate ARS and upgrade SSADARS equipment as well as expand from 3,700 to 4,600 terminals. In addition, future plans could involve as many as 35,000 terminals. We believe that expansion plans must include systems changes to correct existing security deficiencies to protect a valuable national resource.

STEPS TAKEN BY SSA TO IMPROVE SECURITY

On December 17, 1976, we briefed the Commissioner of SSA on our preliminary observations. We emphasized that field offices have had to devise their own security procedures concerning automated beneficiary records without use of any SSA-wide policy or guidelines. We further advised the Commissioner that the degree of security within field offices varied among installations, and that there was a lack of control over use of the terminals for the telecommunications system.

After our briefing, SSA took the following steps to improve security over access to terminals and data included in the telecommunications network.

--Authorized regional commissioners to purchase about 200 doors and 480 locks for rooms where inputting terminals are kept. (According to SSA, all but 11 offices have obtained locks and doors as of December 1977.)

--Instructed offices to limit access to these rooms to authorized employees.

--Instructed offices to keep rooms locked when not in use or whenever authorized personnel are not in a position to observe or control access to the room.

In February 1978, SSA started a pilot study to test the feasibility of using personal identifiers within the telecommunications system to restrict employees to a certain predefined set of transactions. This approach would include a document identification number and a personal identification number with each transaction, and would serve as an audit trail. With this capability, the security system would be better able to restrict employees to either input or query functions according to their assigned duties and responsibilities.

SSA is also considering several other modifications to system security measures (see app. III) which would allow the agency to

--monitor and report unauthorized attempts to use terminals,

--verify the right of access to automated files by various users,

--monitor and report high-risk transactions, and

--improve the lock/unlock procedures.

AUDIT REPORTS ISSUED BY HEW

Concurrent with our review efforts at field offices, the HEW audit agency was performing reviews of the SSA automated telecommunications network. Its reviews were performed primarily at SSA headquarters and other Federal agencies having access to the ARS system. During May and June of 1977, this agency issued two reports to SSA concerning security controls on terminals used on the network, and reported several security weaknesses to SSA that needed immediate corrective action. In summary, the audit agency reported that:

--Management emphasis on security had been too limited. Until the time of its review, very limited SSA-wide security procedures had been issued.

--About half of the computer terminals installed at SSA headquarters were in areas that could not be locked up at night, thus possibly allowing unauthorized access to terminals.

--Many employees knew the passwords which lock/unlock the terminals and were given access to personal information, though their jobs did not require such knowledge or access.

--Reports to regional offices on possible violations of computer security were too late to be useful and often inaccurate.

--The computer programs designed to provide additional security were ineffective in blocking unauthorized use of the system.

--With basic knowledge of the system, it is possible for claims data to be entered into the SSA system from an ARS terminal located in other Federal and State agencies or private insurance companies. To stop this, SSA made arrangements with GSA to ensure that only SSA devices can input data to the Headquarters Computer Facility.

SSA concurred with the audit agency's findings and agreed to take corrective action. As indicated in this report, SSA has taken action to correct problems identified by the HEW audit agency.

CHAPTER 3

LIMITED SAFEGUARDS ARE PROVIDED TO PROTECT DOCUMENTS SUPPORTING BENEFICIARY CLAIMS

SSA field offices, private insurance companies, and State Disability Determination Services, 1/ need to provide better protection over documents in files supporting beneficiary claims. There are thousands of these files in most offices, and they contain personal data on beneficiaries such as earnings records, financial status, and medical evaluations. (See app. I.) These files serve as the foundation of a valuable resource of information for the Government and beneficiaries, and they are not being properly safeguarded from potential loss, destruction, abuse, or misuse.

SSA, through the issuance of various regulations and guidelines has expressed concern over the confidentiality of beneficiary data. In addition, other directives have been issued concerning specific security problems as they occur. Contractual agreements with State agencies and insurance companies contain sections pertaining to the confidential nature and limitations on use of records. The agreements state that the contractor will adopt policies and procedures to ensure that information will be used solely for administering the various programs. We found, however, that SSA had not issued any guidelines or criteria for estabishing overall physical security measures at field offices. Moreover, inadequate guidelines have been issued on safeguarding the documents in the files being processed within these offices.

LACK OF EMPHASIS ON PHYSICAL SECURITY BY SSA

The lack of agencywide guidance has left local managers in field offices to their own devices in evaluating and implementing physical security procedures (guard service, burglar alarms, fire protection, etc.). Also, SSA policy allows for the sacrifice of certain degrees of security over documents supporting beneficiary records in order to maintain an acceptable level of productivity.

1/ These organizations are referred to as field offices throughout this chapter.

Field offices included in our review had not developed written procedures regarding physical security for their installation. In some offices, we found 24-hour guard service, burglar alarms, and central fire alarms; while others had none of these services. (See app. II.) It appears that security measures are taken as a result of specific problems as they occur. For example, one SSA district office found it necessary to hire two armed guards before, during, and after working hours because of large and sometimes hostile crowds of claimants. Another office finally installed fire extinguishers in the office after having three fires.

At the time of our review, most field offices had designated security officers, but none of them had received SSA central office or regional office training on security matters. (See app. II.) In 11 offices, the security officers were only responsible for making sure the terminals were locked during nonworking hours.

In most offices, we observed a lack of procedures to control the use and storage of the valuable information in claimant files. (See app. II.) This lack of control can be attributed to (1) placing emphasis on productivity, rather than safeguarding files and (2) relying on other physical security measures for the offices, rather than using locked filing cabinets or other methods of protecting claimant files.

CLAIMANT FILES NOT PROPERLY SAFEGUARDED

We found, for the most part, employees within the field offices have unlimited access to claimant files. Access to these files is not based on a "need to know."

Generally, loose control was exercised over claimant files, i.e., there were no log-out and log-in procedures to identify the location of a claimant's file during the various stages of processing in field offices. Officials at eight offices told us that at times, claimant files cannot be located when needed to process claims. In many instances, however, these files show up at a later time. For example, SSA reported that one beneficiary had occasion to visit the district office some 5 years after original entitlement. In an effort to help the district office, he brought along his SSA claims folder, which somehow had been given to him. District office officials told us that claimant information is generally re-created in cases where claimant files cannot be found for a long period of time.

Most offices have photocopy machines. Field office officials told us that these machines are not secured during nonworking hours. These machines are generally dispersed throughout working areas within an office. Should an employee or some outside intruder decide to obtain claimant information, copies of pertinent documents could be made and removed from the office without any indication that someone had tampered with the file.

SSA's central office reproduces certain eligibility information from the computerized beneficiary records onto microfiche and/or microfilm every 3 months. Each district and branch office receives copies of these records pertaining to beneficiaries living in its geographic area. Most offices have microfiche reader/printers capable of reproducing individual claimant records in hard copy. The records can be interpreted by using a manual provided by SSA's central office. We observed that these manuals were not secured and were generally stored next to the microfiche readers.

Many SSA offices have more than one set of microfiche files. Some are stored in locked cabinets; however, others are kept on a circular file which cannot be locked. The lockable cabinets can be closed and secured with a padlock, but not all field offices lock these cabinets during nonworking hours. An official at one office told us that these locks would not be a deterrent to anyone who wanted to illegally obtain beneficiary information. We determined that an intruder could reach through the locked cabinet and obtain files or could turn the case upside-down, causing all files to fall to the floor. These microfiche files are available for use and reproduction by all employees. A reader and reproduction unit is available in each office. Files and reader and reproduction units are located in open areas of the office.

Offices generally had been furnished file cabinets for storage of claimants' folders. However, in most cases only employee personnel records were stored in locked cabinets. Claimant files were stored in metal file cabinets, cardboard transfer boxes, and on employees' desks.

Claimant files were generally located in unsecure areas in the office. One region's officials told us that since the advent of SSI, field offices have not had enough lockable file cabinets to store the great number of folders, and that many files had to be left out in the open overnight. Field

officials further stated that the productivity of employees would be reduced if claimant files were put away each night in locked cabinets. In a study conducted by SSA, it was found that about 30 percent of the field offices follow a clean desk policy--they put folders in file cabinets during nonworking hours.

PHYSICAL SECURITY OVER FIELD INSTALLATIONS NEEDS IMPROVEMENT

The implementation of physical security measures has been the responsibility of each local office manager. We found little evidence that any of the offices visited had formally studied the need for physical security measures, or had developed formalized contingency plans to back up their operations if a loss or disaster should occur.

Access to field offices

Most of the over 1,300 offices throughout the country are located in space that is leased by the Government. Landlords for such space generally retain keys to the offices.

We found that 15 offices did not have guard service nor burglar alarms to prevent illegal intrusion during nonworking hours. These offices rely on securable windows and/or doors and controls of keys to prevent illegal intrusion. One office had an alarm system on each door and motion detectors on the ceiling. Another office had an alarm system on each door and a television camera with a viewer to scan the parking lot.

Some field offices in urban centers have guards on the premises during working hours. Some offices have 24-hour guard service, which is provided by their building owner; while others rely on local police protection.

We noted that some field offices have been burglarized. At one office, thieves broke through the front windows and stole two electric typewriters and three calculators. At another office, intruders entered the office through air ducts in the ceiling and took two cassette tapes. Moreover, another office was burglarized, and a SSADARS terminal was stolen together with typewriters, an adding machine, and other equipment.

In many offices visited, we observed little control over the keys to the office. In leased facilities, owners retain keys, and their janitorial services, which need

access to the offices during nonworking hours, also have keys. Office managers are responsible for establishing controls over use of keys to the office. Although some managers maintain a list of key holders, these lists vary in that they include as many as all employees in the office or only select management personnel. Additionally, we found only one office that used keys marked to indicate that they should not be reproduced.

Protection from losses caused by fire

As shown in appendix II, most offices rely on hand fire extinguishers for protection against losses caused by fire. In some instances, these extinguishers are located outside the immediate office. Moreover, many of the offices do not have central fire alarm systems. This situation leaves the office vulnerable to fire losses (both claimant records as well as equipment).

While visiting one office, we noticed many weaknesses in fire protection, access control, and in general, physical security measures for the installation. On April 1, 1977--after our visit--this office suffered extensive fire damage, and some claimant records and valuable equipment were lost and had to be replaced. Estimated loss from the fire exceeded $24,500. The fire department was notified by a passerby, and we were told by officials of the local police department that, had the fire gone undetected for another half hour, the intensity of heat buildup within the office would have ignited many of the 3,500 hard copy files stored in desks and file cabinets.

This is the third fire, believed by the City Fire Marshall to have resulted from arson, at this office since January 1, 1977. The two earlier fires occurred in the office supply room during nonworking hours and damaged some equipment, SSA forms, and other paper goods stored in the area. After each of the three fires, the local police department advised the office that physical security measures needed to be improved. However, no action was taken until after the fire on April 1, 1977. The office has since installed hand fire extinguishers as well as locks on windows and doors.

Disposal of waste paper

SSA's central offices had not issued instructions concerning disposal of documents containing beneficiary information. We noted that practices for waste paper disposal varied among the offices visited. Supervisors and managers

rely primarily on the discretion of individual employees when disposing waste paper. Those who are aware of documents containing beneficiary information generally tear them before throwing them away. However, others do not. In waste cans, we found copies of queries and other documents containing beneficiary information that had not been mutilated.

Most offices had trash disposal service that picked up the trash periodically. Some office managers were not aware of the method of disposal (incinerator or landfill dumps, etc.) once the trash was removed from the offices.

Problems with disposal of waste paper have also been identified by SSA. For example, in September 1976, SSA reported that:

> "Any number of data listings containing all kinds of information which have been seen in paper reclamation centers, on loading docks, in dumpsters and simply lying in SSA halls."

OTHER PROBLEMS IN SAFEGUARDING BENEFICIARY INFORMATION

Safeguarding beneficiary data when answering telephone requests

SSA provides beneficiaries information over the telephone. One SSA regional official said SSA provides telephone service to better serve its clients, and we believe this helps to decrease the number of people visiting the field offices.

We made telephone calls to 46 field offices during our review. Posing as welfare workers, spouses, relatives, and private citizens, we tried to obtain addresses, payment, and eligibility information on certain SSI recipients. In only 4 out of 46 instances did we acquire information on beneficiaries.

Posing as a social worker, we asked why a beneficiary had not received a Medicaid card. We were asked for his address and social security number, and were subsequently told that he had not received a Medicaid card due to his failure to show up for his eligibility redetermination.

Using the same beneficiary information, we contacted another office, posing as his daughter. We said the elderly beneficiary was disoriented, and asked why he had not received his SSI check. We were requested to furnish his social security number again. We were told the claimant was suspended because he did not get his reevaluation. We were advised to bring him in for a redetermination.

In another instance, we called, posing as a spouse, wanting to know if a beneficiary's SSI check had been reduced. We were told that the check amount had not been reduced; however, we were not told what the amount of the check was.

In another instance, we called, posing as a relative trying to obtain information on a beneficiary's SSI benefit amount. We were told the exact amount of benefits being paid to the individual.

In these instances, apparently something led field office employees to believe we were entitled to the information. However, the same approach to 42 other telephone contacts resulted in a firm "no" for personal information. A majority of employees said the beneficiary had to give permission or consent, as specified in the Privacy Act, before the information could be released.

SSA officials said telephone services might be contrary to security. It is difficult for employees who provide services over the phone to be certain of an individual's identity. Even if the caller provides sufficient personal information, the employee still has no way of verifying whether the caller is actually the beneficiary. They said employees may require more training and instruction on the type of identifiers required before releasing any beneficiary information.

Security background checks on field office employees not normally made

Background checks on employees are not normally made by field offices. (See app. II.) However, one office visited made limited background checks on employees. For the most part, potential employees are hired in the field based on interviews and limited followup of prior employment references. This approach may not always provide the degree of assurance needed when evaluating the integrity of potential employees. For example, SSA has experienced instances where:

--One SSA employee sold information to a company that was in the business of locating missing persons.

--Two SSA field office employees fabricated 14 different beneficiary accounts and processed them for payment. A total of over $55,000 was paid on these accounts before the employees' actions were discovered.

--An employee of a private insurance company which acts as a carrier for Medicaid and Medicare payments reissued several checks that had been previously returned due to the death of the beneficiary. The checks were reissued in another name by the employee and forwarded to various post office boxes for later retrieval.

We believe SSA should identify those employees in sensitive positions and require that background checks be made. Background checks help assure that employees hired for sensitive positions are less likely to be involved in abusing program data.

SECURITY OVER BENEFICIARY INFORMATION SENT TO OTHER ORGANIZATIONS

During our review, we noted potential security problems in safeguarding beneficiary information at other organizations. SSA submits beneficiary information to (1) States for their use in administering their programs, such as welfare, and (2) insurance companies for their use in administering Medicare. The States and insurance companies provide this information to other offices within their organizations. The method of providing such information to the other offices varies and could be via telecommunications, listings, punch cards, or microfilm.

We did not attempt to determine whether adequate security is provided over beneficiary information in these cases. SSA officials told us that they have not extended their review of security to include the security practices of these organizations.

SSA should review the security procedures and practices of any organization receiving beneficiary data (e.g., Federal and State agencies and storage centers, private contractors, etc.). Without proper safeguards, the potential for abuse and misuse of information exists.

- - - -

We believe that beneficiary records are vulnerable to potential abuse and/or misuse and destruction in most field offices because of problems associated with

--the way claimant files are stored,

--the readily available use of microfiche files and photocopying equipment,

--weaknesses in securing field office space after working hours,

--inadequate fire protection,

--the way in which sensitive documents are disposed,

--safeguarding beneficiary data when answering telephone requests,

--security background checks on field office employees, and

--the security practices of other organizations receiving beneficiary information.

SSA ACTIONS TAKEN DURING OUR REVIEW

As mentioned on page 12, we briefed the Commissioner of SSA on our preliminary observations on December 17, 1976. Our preliminary observations showed that:

1. SSA had not developed security guidelines for documents and files supporting beneficiary claims.

2. An ad hoc group had been established to study the area of security but had not issued any definite instructions to field offices.

3. Security officers had been designated in most field offices; however, they had not received any training.

4. Local offices had established their own security procedures.

5. Physical security measures in offices varied from simple locked doors to use of motion detectors.

On February 4, 1977, the Associate Commissioner for Program Operations commented on our preliminary observations by stating this:

"* * * The ad hoc group referred to in the GAO observations is now a permanent staff (Systems Security Staff) attached to the Office of Program Operations. * * *"

After our briefing, the Systems Security Staff prepared several publications and took certain actions on security matters. For example, certain material has been distributed to field offices, and other actions, such as the following, have been taken since February 1977.

--Lesson Plan--"Privacy Act of 1974" (distributed in February 1977).

--Pamphlet--"Systems Security Question and Answers" (March 1977).

--Booklet--"Why System Security" (April 1977).

--Booklet--"Glossary of Systems Security Terms" (April 1977).

--Video Tapes (April 1977).
  a. "Whose Right to Know."
  b. "Follow that card."
  c. "Systems Security and You."
  d. "Physical Plant Security."

--Portions of eight chapters and the Table of Contents of the System Security Handbook have been issued to all regional and central office component security officers between May and September 1977.

--Audits of security matters covered in this report have been conducted at about 200 field offices between June and December 1977. SSA plans a followup review at all offices at least once each year.

--Security audits have been conducted of certain central office components during November 1977.

--SSA conducted a study of computer-related crime vulnerability in the Supplemental Security Income System and published its report in October 1977. (This was the first program-oriented study conducted by SSA). SSA plans to conduct a similar study for other major systems during 1978. Problems identified in this study confirm our observations during the review. SSA issued guidelines on disposal of waste paper during August 1977.

Regional security officers meetings were held during May and November 1977. These meetings included discussions on systems security and privacy matters.

In July 1977, the Secretary of HEW requested a list of major operational priorities to achieve tangible improvements in services provided clients.

The Commissioner of SSA replied on October 12, 1977. One of the major priorities included an SSA-wide system security program, which included a statement that:

"Although these many projects are under way, system security is still in its developmental stages. As we gain more experience with the function and study both industry and other Government agency programs, we expect to identify new approaches, and in turn, to develop and employ new security measures."

In a meeting held on November 9, 1977, with SSA management, the Secretary of HEW recognized the importance of this major priority. We believe this is a big step in improving the system's security program.

In addition, during April 1978, SSA held a symposium on privacy and security. This meeting included a group of experts in the field of computer security and workshop discussions on specific problems unique to the SSA operation.

CHAPTER 4

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

In fiscal year 1977, SSA's electronic data processing system serviced over 33 million beneficiaries receiving about $103 billion annually. With the vast number of records, and the number of offices involved in the SSA operations, safegaurds must be present to prevent unauthorized alterations, destruction, abuse, or misuse of beneficiary records--a valuable national resource. Millions of individual records are involved, and thousands of employees in field offices have access to these records through a vast telecommunications system.

This report demonstrates that SSA did not have an active security program which would assure the Congress, the public, and beneficiaries that records maintained by SSA were adequately safeguarded. However, since our review began, SSA has started an active security program.

We found several management weaknesses in the SSA computer network, such as

--the ability to create as well as query beneficiary files from most terminals,

--the failure to use the audit trail features within the system,

--the failure to always lock terminals during nonworking hours, and

--the unlimited and unrestricted access to terminals.

Also, hard copy beneficiary records are vulnerable to potential abuse and/or misuse and destruction in most field offices because of problems associated with

--the way claimant files are stored,

--the readily available use of microfiche files and photocopy equipment,

--weaknesses in securing field office space after working hours,

--inadequate fire protection,

--the way in which sensitive documents are disposed,

--safeguarding beneficiary data, and

--security background checks on field office employees.

Safeguarding records given to State agencies through various exchange programs also presents potential security problems.

During our review, SSA started an active security awareness program designed to strengthen procedures used to safeguard various records. It appears that SSA has recognized the importance of protecting these valuable records.

RECOMMENDATIONS

In view of the cited weaknesses in the telecommunications network and SSA's plans to expand the network, we recommend that the Secretary of Health, Education, and Welfare direct the Commissioner of Social Security to take the following actions immediately.

--Restrict terminals located in open areas of district offices to queries only.

--Provide secure rooms for the printers, and consider the feasibility of having all printed output monitored and distributed by data transmission personnel.

--Restrict the ability to create records or to access the national data base to only that data necessary for each specific class of office.

--Restrict the ability to create records or make changes to existing records in accordance with employee and maintenance personnel duties and responsibilities by requiring a unique and personal identifier for every data transmission.

--Provide a personal identifier on input documents for the person who performs the interview, prepares input documents, and reviews input documents and supporting documentation.

--Restrict knowledge of the password used to lock and unlock a terminal to the office manager, assistant manager, and security officer.

--Require this password to be changed at least monthly, and whenever any employee knowing the password is no longer employed at that office.

--Require that any expansion of the existing telecommunications system include system changes to correct security deficiencies.

The Secretary of HEW should continue to pursue an active and aggressive security program to assure the Congress, the public, and SSA beneficiaries that records are properly safeguarded against abuse, misuse, destruction, or alteration. In this effort, the Secretary should conduct a risk analysis to determine how best to correct the security weaknesses identified in this report and determine whether other security weaknesses exist. The effort should include security measures in terms of efficient and effective services to beneficiaries--a balance between good service and good security should be weighed.

APPENDIX I

BENEFICIARY INFORMATION STORED IN OR AVAILABLE TO FIELD OFFICES AND STATE AGENCIES

INFORMATION CONTAINED IN SSI CLAIMS FOLDERS

1. Application for SSI, which includes the claimant's name, social security number, date of birth, address, public assistance history, assets, and other property.
2. Statement of Income and Resources, which lists wage amounts, unearned income, real estate, and other property and resources (cash, bank accounts, and savings).
3. Copy of the microfiche file, if receiving SSI benefits.
4. SSI payment worksheet, which computes the payment amount.
5. SSI Claim Review Record, which shows payment status and amount.
6. SSI Continuing Determination Statement.
7. Notice of changes in payment amount.
8. SSI queries, which show up-to-date status of claimant's account, mortgage papers, and loan agreements.
9. All other forms, report of contracts, and correspondence that relates to the claimant's case.

INFORMATION CONTAINED IN TITLE II AND RETIREMENT AND DISABILITY INSURANCE CLAIMS FOLDERS

1. Application for retirement or disability insurance, which lists the claimant's address, marital status, social security number, date of birth, employers, and disability.
2. Earning Record and Primary Insurance Amount Computation, which lists total earnings counted towards Social Security coverage and specifies the amount the claimant would receive if retired or disabled.

3. Request for Medical Evidence, which is a request to the claimant's doctor for medical information.

4. Report of Disability Interview, which is a claimant's description of the disability as told to an SSA employee.

5. Disability Determination Sheet, which indicates if a claimant is disabled and at what date the disability began.

6. Document supporting date of birth and annual estimates of income Doctor's comments, letters, and medical reports, which describe the claimant's condition in medical terms.

7. All other forms, report of contacts, and correspondence that relates to the claimant's case.

LISTING OF SOME INFORMATION AVAILABLE TO SSA OFFICES AND STATE AGENCIES FROM THE TELECOMMUNICATIONS NETWORK (ELIGIBILITY INFORMATION IS REPRODUCED ON MICROFICHE EVERY 3 MONTHS)

Applicant's:

--Last name.
--Address.
--Social Security number
--Drug addict or alcoholic code.

--Date of Disability Onset.
--Denial Code.
--Date of Birth.
--Representative Payee.

--Income from Self-Employment.
--Income from wages.

--Entitlement Code.

--Federal living arrangement code.
--Federal SSI monthly assistance amount.

--Marital status code.

--Monthly benefits from retirement program.
--Medicaid effective date.
--Payment status code.

APPENDIX I

--Race code.

--Recipient Bank account, number, and account identifier.

--Representative payee custody code.

--Sex code.

--Telephone number.

--Unearned income amount.

--Welfare number.

APPENDIX II

PROFILE OF SECURITY PRACTICES AT SELECTED INSTALLATIONS PROCESSING SSA AND MEDICARE DATA

SECURITY MEASURE \ INSTALLATION	SSA INSTALLATIONS																							STATE DISABILITY OFFICES								INSURANCE COMPANIES			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
TYPE OF SPACE OCCUPIED:																																			
Government-Owned Space	●										●	●				●																			
Rented/Leased Commercial Space		●	●	●	●	●	●	●	●	●			●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
PHYSICAL SECURITY OF STRUCTURE:																																			
Access Restrictions:																																			
Security Guards for Office:																																			
Working Hours	○	●	○	○	○	○	●	●	●	○	○	●	●	●	○	●	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	●
Non-Working Hours	○	○	○	○	○	○	○	●	○	○	●	●	○	●	○	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	●
Security Guards for Building	●	●	○	●	○	○	●	●	●	○	●	●	○	●	○	○	●	○	○	○	○	○	●	○	○	●	○	○	○	○	○	○	○	○	●
Receptionist	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	○	○	○	○	○	●	○	○	●	○	○	○	●	●	●	○	○	●
Burglar Alarms	●	○	○	○	○	○	●	○	○	○	●	○	●	○	○	○	○	●	●	○	○	○	●	○	○	○	○	●	○	●	○	●	●	●	●
Door Locks:																																			
Office	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Machine Room	○	○	●	●	●	●	●	○	○	○	●	●	○	○	●	●	●	○	○	○	●	○	○	●	○	●	●	●	●	●	●	○	○	○	●
Hanging Ceilings with Partial Walls	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	●	●	●	●	●	●	●	○	●	●	○
Securable Windows	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	○	●	●	●	●	●	●	○	●	○[1]	●	●	●	○	●	●	●	●	●
Control Over Keys to Office[2]	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	●	●	●		○	○	●	●	○	○	○	○	●	●	●	●
Fire Protection:																																			
Central Fire Alarm System	●	○	●	●	○	○	●	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○	●	○	○	●	○	○	●	●	○	●	●	●	●
Smoke Detectors for Office	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	○
Sprinkler System in Office	○	○	○	○	○	○	●	○	●	○	○	○	●	○	○	●	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Hand Extinguishers:																																			
Within the Office	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Within the Building	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
PERSONNEL WORKING WITHIN THE OFFICE:																																			
Employee Background Checks for Security Performed	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Supervision of Maintenance Staff:																																			
Government Employees											○	○	○			○							○												
Contractor Employees	○	○	○	○	○	○	○	○	○	○			○	○	○		○	○	○	○	○	○		○	○	●	○	○	●	○	○	○	○	○	○
SECURITY OFFICERS:																																			
Security Officer Designated	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●
Defined Duties and Responsibilities	○	○	○		○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	○	●	○		○	○	○
Trained in Security Matters	○	○	○		○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○
Extent of Responsibility:																																			
Automated System Only	○	○	○		●	●	●[3]	●[3]	○	○	○	●	●	○	○	●	●	○	○	○	●	○	●[3]	●	●	○	●	○	○	○	○		○	○	●
Office-Wide (Including Automated System)	●	●	●		○	○	●[3]	●[3]	●	●	●	○	○	●	●	○	○	●	●	●	○	●	●[3]	○	○	●	○	●	●	●	●		●	●	○
HARD-COPY BENEFICIARY FOLDERS:																																			
Procedures for Restricting Use:																																			
During Working Hours	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			○	○	○	●	○	○	○	○	○	○	○	○	○
During Non-Working Hours	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			○	○	○	●	○	○	○	○	○	○	○	○	○
Controls Over Use of Photocopiers	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	●	○	○	○	●	○	○	○	○	●	○	○	○	○

KEY TO PROFILE

● = Yes

○ = No

□ = Not Applicable

NOTES:

1. Office occupies 13th and 14th floors of building. Windows cannot be accessed easily.
2. Internal control of keys for employees within the office. This control did not always extend to landlords and contractor maintenance employees.
3. Office has two security officers: One responsible for the automated system only; and the other responsible for office-wide security matters.

APPENDIX II

PROFILE OF SECURITY PRACTICES AT SELECTED INSTALLATIONS PROCESSING SSA AND MEDICARE DATA

SECURITY MEASURE \ INSTALLATION	SSA INSTALLATIONS																							STATE DISABILITY OFFICES								INSURANCE COMPANIES			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
HARD-COPY BENEFICIARY FOLDERS (CON'T):																																			
Storage:																																			
Open Space (e.g., Desk Tops)	○	●	○	○	●	●	○	●	●	●	○	●	●	●	●	●	●	●	●	○	[4]	[4]	●	○	○	○	○	○	●	○	●	●	●	●	●
Locked File Cabinets	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			○	●	●	●	●	●	●	○	●	○	○	○	●
File Cabinets without Locks	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	○	●	○	●	●	●	●	○	●	●	●
Open Storage Bins																													●		●	●		○	
Disposal:																																			
Destructive Device Used	○	○	○	○	○	○	○	○	○	●	●	○	○	●	●	○	○	○	○	○	○	○	○	○	●	●	○	○	●	●	○	●	○	○	●
Paper Shredding Machine										●	○			●	○										●	○			●	●		●			●
Hand Paper Cutter										○	●			○	●										○	[5]●			○	○		●			●
AUTOMATED BENEFICIARY FILES:																																			
Location of Terminals:																																			
All in One Room	○	○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○	●	●	○	○	○	○	●	●	●	●	●	○	●	●	●	●	●	●
Dispersed Throughout Office	●	●	●	●	●	●	○	●	●	●	○	●	●	●	●	●	●	○	○	●	●	●	●	○	○	○	○	○	●	○	○	○	○	○	○
Terminal Located at Main Office Entrance	○	○	●	●	○	○	○	●	●	○	○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Control over the Use of Terminals:																																			
Input of New Information	○	○	○	○	●	●	○	●	○	○	●	●	●	●	●	●	○	○	○	○	●	●	●	●	●	○	○	●	●	●	●	●	●	○	●
Querying Beneficiary Files	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	○	○	●	●	○	●	●	●	○	●
Personal User Identification Required	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Frequency for Changing System Passwords:																																			
Daily							●				●																							[6]	[6]
Weekly	●															●													●						
Monthly														●																					
Quarterly		●																			●				●										
Semi-Annually			●	●							●						●	●	●	●		●													
Annually								●	●						●								●				●				●				
Turnover of Employees that are Knowledgeable of the Password										●													○												
Not Changed				●	●						●															●		●			●		●		
Access Restrictions to Machine Room	○	○	○	●	●	●	●	○	○	○	●	○	○	○	●	○	○	○	○	○	●	○	○	○	○	●	○	○	●	○	○	●	○	●
System Manuals Secured	○	○	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	●	○	○	●	○	○	●
Controls Over Use of Printer	○	○	○	○	●	●	○	○	○	○	○	○	○	○	●	○	●	○	○	●	○	○	●	●	●	●	●	○	●	○	●	○	●	○	●
MICROFICHE/MICROFILM FILES: [7]																																			
Controls Over Use of Files	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			○		○		●				○
Files Dispersed Throughout Office	●	●	●	●	●	○	●	●	●	●	●	●	●	○	●	●	○	○	○	○	●	●				○		●						○
Reproduction Machines Nearby	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●				●		●		●				
DOCUMENTED SECURITY PROCEDURES:																																			
Contingency Plans and Backup Procedures	●	●	○	●	○	○	●	●	●	●	●	○	○	●	●	●	○	●	●	○	○	○	○	○	○	●	○	C	●	●	○	●	○	○	○
Automated Systems	○	○		○			○	○	○	○	●			●	●	○		●	○							○			●	○		○			
Personnel Safety	●	●		●			●	●	●	●	●			●	●	●		●	●							●			●	●		●			
System Lock/Unlock Procedures	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	○	○	○

KEY TO PROFILE

- ● = Yes
- ○ = No
- □ = Not Applicable

NOTES:

4. These are teleservice centers which do not store hard copy beneficiary folders.
5. Hand paper cutters not always used to destroy hard copy beneficiary information.
6. Offices do not use the Lock/Unlock procedures.
7. Microfilm/microfiche records stored in State Agencies and insurance companies are not produced by SSA but they contain beneficiary information.

IMPROVEMENTS MADE OR PLANNED BY SSA TO STRENGTHEN CONTROL OVER THE USE OF TERMINALS 1/

SSA is in the process of making modifications to security procedures which, according to the systems security staff, will allow the agency to:

1. Monitor and report unauthorized attempts to use terminals

"The software filter." better known as the "security matrix," limits SSADARS and ARS terminal functional units to a specific set of transactions. Attempted transactions, not included in the set of transactions allowed an operating unit, are rejected as unauthorized. A report associated with the SSADARS Security Report Sytem monitors the incidence and occurrence of unauthorized transactions.

Currently, the SSA Systems Security Officer has the authority and responsibility to maintain an ongoing evaluation of the SSA Security System Transaction Register associated with the "security matrix." This responsibility involves establishing the appropriate functional data access level ("security level") of each operating component. To aid him in this function, the Bureau of Data Processing, in conjunction with the SSA Systems Security Staff, is currently evaluating possible modifications to the SSADARS Security System Transaction Register. This evaluation will consider the possible restriction on the use of "free-form" transaction verbs, such as "AA and SS."

2. Verify the right of access to automated files by various users

"Validation of each functional components' transaction capability and security level is currently in process. The object of this project is to establish the exact transaction capability needed by each operating component. Once the validation is completed, each

---

1/According to "SSA Sytems Security--Major Projects and Goals" (May 13, 1977).

APPENDIX III

operating unit will be intrinsically associated through a 'benchmark' tape to operating programs. Our plan is to compare program (SSI, etc.) transactions associated with a functional unit over a given period of time with the units established benchmark transaction tape. This comparison would reveal both inconsistencies in transaction security and outright program compromise.

"Currently, various aspects of the telecommunications system are monitored by the SSADARS Security Report System. This system produces reports associated with 'alt mode' transactions, attempted unauthorized transactions and the use of the lock/unlock software feature. In the future, the SSADARS Security Report System, which also monitors certain ARS transactions, will be expanded to provided daily reports on a varied number of activities directly to system managers.

"It is conceivable that specific programs such as IMPACC and OTP could be monitored by connecting transaction to initiator. It has been proposed that reports concerning these programs could be directed via telecommunications terminals to the appropriate security officer."

3. Monitor and report high-risk transactions

"A resident audit system to monitor high risk transactions has been proposed and is in the process of being developed. The objective of this system is to monitor activity surrounding transaction * * *."

"Based on experience dealing with computer crime and in evaluating systems vulnerabilities, the two most likely methods that can be used to obtain fraudulent payments are creating a fictitious recipient record or changing an address instead of terminating an

existing record. As a result, the resident audit system will be geared to monitoring these transactions, especially when asssociated with the SSI program."

4. Improve the lock/unlock procedures used to close terminals in field offices

"This is to announce a change to the telecommunications lock and unlock system which will obviate the bulk of the problems experienced by operators attempting to use the lock/unlock procedures when the central system is down.

"Effective May 23, 1977, if a 'lock' request is entered and cannot be delivered to central computer operations in Baltimore, a spool receipt will be returned to the originating screen indicating 'LOCK PENDING - RECEIPT WILL BE ROUTED TO PRINTER.' The actual 'lock' request will be stored in the local concentrator until the system comes up. When this occurs, the 'lock' will be transmitted to the central computer on a priority basis. The subsequent receipt will be delivered to the SSADARS printer associated with the originating terminal.

"The ARS stations with 'online' access capability will also be affected by this feature. In the event a 'lock' request is entered from an ARS terminal and cannot be delivered to the central computer, a receipt message will be returned indicating 'LOCK PENDING.' The 'lock' request will be stored in the concentrator until communications with central computer operations can be reestablished. When this occurs, the 'lock' will be transmitted to the central computer on a priority basis. No subsequent message will be returned to the ARS station indicating that the lock has subsequently taken affect. However,

the assumption should be made that the terminal will be locked once communications are reestablished.

"It should be noted that in the very rare instance that an outrage occurs at the concentrator prior to transmitting the 'lock' to the central computer, the message will be lost. Again, this will occur on rare occasions and should not detract from the enhanced efficiency of the SSADARS/ARS 'lock' feature."

PRINCIPAL OFFICIALS

RESPONSIBLE FOR ADMINISTERING

ACTIVITIES DISCUSSED IN THIS REPORT

	Tenure of Office	
	From	To
SECRETARY OF HEALTH, EDUCATION, AND WELFARE:		
Joseph A. Califano, Jr.	Jan. 1977	Present
David Mathews	Aug. 1975	Jan. 1977
COMMISSIONER OF SOCIAL SECURITY:		
Donald I. Wortman (acting)	Dec. 1977	Present
James B. Cardwell	Sept. 1973	Dec. 1977
ADMINISTRATOR OF HEALTH CARE FINANCING ADMINISTRARTION:		
Robert A. Derzon	June 1977	Present
Donald I. Wortman (acting)	Mar. 1977	May 1977