

19728

116779

REPORT BY THE U.S.

General Accounting Office

RELEASED

RESTRICTED — Not to be released outside the General Accounting Office by the Office of Congressional Relations

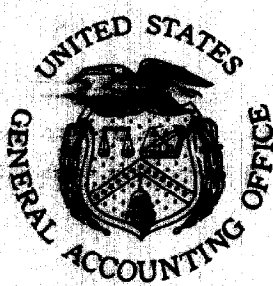
RELEASED

Procedures To Safeguard Social Security Beneficiary Records Can Still Be Improved

In 1978, GAO pointed out to the Social Security Administration (SSA) weaknesses in its security over beneficiary records and recommended that they be corrected. SSA agreed to take action. GAO reviewed SSA actions and found that two of the nine recommendations have been implemented, and seven of the recommendations are in various stages of implementation. GAO recommends that the Secretary of the Department of Health and Human Services (HHS) direct the Commissioner of Social Security to give priority to implementing the recommendations. GAO also recommends that the Secretary of HHS require SSA to evaluate the current role of its System Security staff and, if deemed necessary to achieve an aggressive security program, establish within SSA one office with the responsibility, capability, and authority for implementing such a program.



116779



HRD-81-157
SEPTEMBER 30, 1981

518885

Request for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Document Handling and Information
Services Facility
P.O. Box 6015
Gaithersburg, Md. 20760**

Telephone (202) 275-6241

The first five copies of individual reports are free of charge. Additional copies of bound audit reports are \$3.25 each. Additional copies of unbound report (i.e., letter reports) and most other publications are \$1.00 each. There will be a 25% discount on all orders for 100 or more copies mailed to a single address. Sales orders must be prepaid on a cash, check, or money order basis. Check should be made out to the "Superintendent of Documents".



UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

HUMAN RESOURCES
DIVISION

B-200202

The Honorable Max Baucus
United States Senate

The Honorable Orrin Hatch
United States Senate

The Honorable Charles Rose
House of Representatives

On June 5, 1978, we issued a report entitled "Procedures to Safeguard Social Security Beneficiary Records Can and Should Be Improved" (HRD-78-116). Our report identified security and management problems which could lead to potential loss, destruction, abuse, or misuse of beneficiaries' automated and hard copy records maintained by offices using the Social Security telecommunications network--Social Security offices (district, branch, teleservice centers, and program service centers), State disability determination services, and certain Medicare contractors. We recommended that Social Security correct the weaknesses.

Subsequently, you asked us to answer a number of questions, some of which were related to our June 5 report. The questions addressed, among other things, (1) Social Security's actions on our recommendations to correct weaknesses in offices using the telecommunications network, (2) security safeguards over beneficiary data provided to State agencies (other than State disability determination services), through the Social Security data exchange programs (not the Social Security telecommunications network), and (3) several matters relating to Social Security beneficiary data given to other Federal agencies.


During a series of meetings with your offices, it was agreed that we would respond to your request by (1) answering the questions relating to Social Security's actions on our recommendations, beneficiary data exchanged with other Federal agencies, and certain other questions relating to additional detailed information in one report; (2) answering questions relating to safeguards over beneficiary information given to other State agencies through data exchange programs in a second report; and (3) briefing your offices on the results of our efforts regarding the other questions. A

briefing addressing these questions was held on March 18, 1981. This report addresses the question concerning the Social Security Administration's (SSA's) actions on June 1978 recommendations, data exchanged among Federal agencies, and additional detailed information (question (1)). In another report, we are responding to the matters raised by the question concerning State agencies (question (2)).

Representative Rose requested Social Security to provide him with answers to questions similar to those you posed to us, and as agreed with your offices, we have answered the questions dealt with in this report primarily by determining what actions SSA has taken or plans to take in connection with our June 1978 recommendations.

As agreed with your offices, we did not obtain formal agency comments on our draft report; however, we discussed its contents with officials responsible for security in SSA and have incorporated their comments where appropriate.

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


Gregory J. Anart
Director

D I G E S T

WHY THE REVIEW WAS MADE

In June 1978, GAO issued a report which identified security weaknesses in protecting beneficiary records maintained in field offices under the stewardship of the Social Security Administration (SSA). GAO made nine recommendations directed toward correcting the weaknesses. SSA agreed and began action to correct the weaknesses. Subsequently, several Members of Congress requested that GAO determine what actions had been taken to implement the recommendations.

FINDINGS AND CONCLUSIONS

As of September 1981, two of the recommendations had been implemented while the other seven were in various stages of implementation.

After GAO pointed out the security weaknesses, SSA recognized that the lack of security over beneficiary records was a problem and established a Systems Security staff, which would have had the authority to implement a strong security program for maintaining beneficiary records. In January 1979, however, the Systems Security staff was reassigned to a position of having to obtain the cooperation of several SSA operating components to develop and implement an adequate security program to protect beneficiary records.

GAO believes that unless there is an office within SSA with the responsibility and authority for developing, implementing, and managing a security program for the protection of beneficiary records, the achievement of such a program may very well be hindered.

RECOMMENDATIONS TO THE SECRETARY
OF HEALTH AND HUMAN SERVICES

GAO recommends that the Secretary direct the Commissioner of Social Security to give priority to implementing the June 1978 recommendations.

GAO also recommends that the Commissioner of Social Security be required to evaluate the current role of the Systems Security staff and the need for an aggressive security program to protect beneficiary records and, if deemed necessary to achieve such a security program, establish an office within SSA with the primary responsibility, capability, and authority for developing, establishing, and maintaining an aggressive ongoing security program for the protection of beneficiary records.

C o n t e n t s

	<u>Page</u>
DIGEST	i
CHAPTER	
1 INTRODUCTION	1
Background information on our report of June 1978	1
Summary of findings in June 1978 report	4
Objectives, scope, and methodology	5
2 WHAT HAS BEEN DONE TO IMPLEMENT RECOMMENDATIONS	6
Medicare contractors have made some improve- ment in security over beneficiary records since HCFA issued standards	8
Although SSA said it improved security measures, adherence to its issued guide- lines is not consistent	9
Specific recommendations and actions taken by SSA	9
3 WHAT SSA HAS DONE AND PLANS TO DO IN SECURITY	17
Present security program and SSA plans	17
Can the planned security goals and objec- tives be effectively achieved under the present management structure?	20
Conclusions	21
Recommendations to the Secretary of HHS	21
APPENDIX	
I SSA data exchanges with other Federal agencies	22
II Other information requested	24

ABBREVIATIONS

ADP	Automated Data Processing
DDS	Disability Determination Service
GAO	General Accounting Office
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
PIN	personal identification number
SSA	Social Security Administration
SSI	Supplemental Security Income

CHAPTER 1

INTRODUCTION

Our June 1978 report 1/ identified security weaknesses in protecting beneficiary records maintained in field offices under the stewardship of the Social Security Administration (SSA).

Subsequently, several Members of Congress asked us to answer a number of questions. The questions involved (1) SSA's actions on our recommendations to correct certain weaknesses pointed out in our June 1978 report (see chs. 2 and 3), beneficiary information exchanged with other Federal agencies (see app. I), and additional information on security over beneficiary records (see app. II), and (2) the extent of security safeguards over beneficiary data provided to State agencies. 2/ This report addresses the questions in (1).

BACKGROUND INFORMATION ON OUR REPORT OF JUNE 1978

Our June 1978 report was concerned with SSA offices (district, branch, teleservice centers, and program service centers), State disability determination services (DDSs), and private insurance companies (Medicare contractors) using the SSA telecommunications network. During that review, we evaluated security procedures used by these offices related to both the automated beneficiary records as well as the documents supporting beneficiary claims. Our report identified security and management problems which could lead to potential loss, destruction, abuse, or misuse of these beneficiary records maintained by SSA. To correct these cited security weaknesses, we made nine recommendations.

The offices covered by our June 1978 report performed the following in administering various programs. Because questions have been raised as to why beneficiary data are being given to DDSs and private insurance companies, we have explained the legislative

1/"Procedures to Safeguard Social Security Beneficiary Records Can and Should Be Improved" (HRD-78-116).

2/We agreed with the requestors that we would (1) respond to the questions on what actions SSA had taken on our recommendations, beneficiary information exchanged with other Federal agencies, and additional information on SSA security in one report; (2) determine and report on the extent of security safeguards over beneficiary information given to State agencies in a second report; and (3) brief the requestors on the results of our work on the remaining questions. We briefed them on March 18, 1981.

requirements to show that the DDSs and private insurance companies need such data to carry out their Federal contractual responsibilities.

Social security offices

There are over 1,300 district and branch offices nationwide that provide personal contact with claimants and beneficiaries. They receive and/or process claims for retirement, survivors and disability insurance, health insurance, supplemental security income (SSI), and black lung benefits. In addition, they process postadjudicative actions on current beneficiaries. Teleservice centers advise the public, and program service centers review and authorize payments or disallow beneficiary claims. These offices are linked to the central complex (headquarters in Baltimore, Maryland) and to each other by a telecommunications network.

State disability determination services

The Social Security disability insurance program is administered under a Federal-State mechanism having its origins in the disability provisions of the 1954 amendments to the Social Security Act. The Congress at that time indicated that determinations of disability should be made by State agencies, under agreements with the Secretary of Health and Human Services (HHS).

Because the Congress was concerned with the problems of rehabilitation and relationships with the medical profession, it indicated that disability determinations under the disability insurance program should be made by State vocational rehabilitation agencies. The Social Security Act, as amended, gave the Secretary of HHS authority to contract with the State vocational rehabilitation agency or some other agency selected by the State to carry out this function. The States are reimbursed by the Federal Government for their costs in making disability determinations.

When an individual applies for disability insurance or SSI disability, the applicant usually goes to the nearest SSA district office where an SSA claims representative interviews the applicant and prepares a medical history and disability report.

The report and any other information developed is then forwarded to the DDS for processing. DDSs use the medical history and disability reports to determine if a disability exists. If, however, a DDS determines that additional information is needed to substantiate the claimed disability for SSI cases, it can obtain information from certain SSA files by using the SSA telecommunications network. This information is available from the Supplemental Security Record (SSI recipients). SSA maintains that

needed information is, for example, (1) trial work periods, (2) medical information related to workers compensation, (3) prior disability, and (4) military medical records.

There are 50 States, Puerto Rico, the District of Columbia, the Virgin Islands, Northern Mariana Islands, and Guam operating under contracts with SSA. The 1981 estimated costs of operating these offices is about \$459 million. In addition, SSA pays for installation and the telecommunications equipment.

Private Insurance Companies (Medicare contractors)

The Social Security Amendments of 1965 established the Medicare program to protect eligible persons, principally those over age 65, against the costs of health care. In 1972, Medicare was extended to persons under 65 who were disabled. Medicare provides two forms of protection (1) Medicare Part A, hospital insurance benefits, and (2) Medicare Part B supplementary medical insurance which covers part of the physician's care and other health benefits.

The Medicare legislation and the accompanying committee reports reflected a congressional decision that program administration be carried out by contracting with private organizations that already serve as third-party payers of health care services and that perform in their private business many functions that they would perform for Medicare. Medicare legislation also intended that a system of local contractors be established that could respond immediately to circumstances where they were already operating and provide maximum personal services to the Medicare beneficiary. It was the Congress' intent that a sufficient number of contractors would be selected on a regional or geographic basis to promote a competitive performance environment and permit comparisons of individual performance.

Title XVIII of the Social Security Act provides that the Secretary of HHS enter into cost reimbursement contracts with contractors to process Medicare claims and make payments on behalf of the Government and that such contracts result in neither a profit nor a loss from carrying out Medicare activities.

The responsibility for administering Medicare rests with the Secretary of HHS. Within HHS, the responsibility has been delegated to the Health Care Financing Administration (HCFA). HCFA contracts with contractors to process Medicare claims and make payments on behalf of the Government. Contractors that pay institutional providers (such as hospitals) are called intermediaries and contractors that pay physicians and suppliers are called carriers. Because the organizations had to make adjustments to their systems

to accommodate Medicare's complex reasonable charge determinations and strict government reporting requirements for a new program, negotiated cost reimbursement type contracts were selected. 1/

The 1981 estimated operating cost for HCFA contractors is about \$694 million. HCFA has entered into 119 agreements with contractors/subcontractors to process Medicare claims.

HCFA relies on contractors to process Medicare claims. The role of these contractors is to determine the amount of Medicare payment due and to make the payment. Because of this role, the contractors need certain beneficiary information to fulfill their contractual responsibilities. SSA maintains the Medicare records and provides support to HCFA through computerized data files and telecommunications capabilities. To facilitate timely claims processing, the contractors use SSA's telecommunications system to inquire about the eligibility of beneficiaries to process the claims in accordance with their contracts. The government pays for the telecommunications equipment and its installation.

SUMMARY OF FINDINGS
IN JUNE 1978 REPORT

Our review showed the following types of telecommunications system design and management problems which led 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 features within the system.
- Failure to lock terminals during nonworking hours.
- Unlimited and unrestricted access to terminals.

We also found that SSA offices, Medicare contractors, and DDSs need to better protect beneficiary files. There are thousands of files in most offices, and they contain personal data on beneficiaries, such as earnings records, financial status, and medical evaluations. They were not being properly safeguarded from potential loss, destruction, abuse, or misuse.

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

1/The Medicare program has three ongoing experiments in Part B that are testing competitive fixed-price procurement in Maine, Illinois, and upstate New York.

We recommended that SSA correct the weaknesses in security and that SSA pursue an active and aggressive security program to assure that beneficiary records are protected. We made nine recommendations directed at correcting the weaknesses. (See ch. 2.)

OBJECTIVES, SCOPE, AND METHODOLOGY

On July 11, 1978, Representative Charles Rose requested SSA to provide him with answers to questions similar to those asked us. In August 1978, SSA responded to Representative Rose and stated it had taken actions to implement two of the nine recommendations. SSA also stated the actions they were taking on the other seven. During meetings with your offices, we agreed to respond to your request primarily by evaluating SSA's response to Representative Rose regarding our recommendations. We reviewed SSA's response regarding the two recommendations and found that, in our opinion, SSA's action satisfied our recommendations. Since then we continuously reviewed SSA's response with SSA officials to make sure the initial answers had not changed. In addition we visited 6 Medicare contractor offices, contacted 13 DDSs, and examined records of SSA security audits of 18 SSA offices. This scope was in accordance with the requestors' instructions, and they were satisfied that the coverage was adequate.

CHAPTER 2

WHAT HAS BEEN DONE TO

IMPLEMENT RECOMMENDATIONS

Our June 1978 report concerned security over beneficiary records in Social Security offices, DDSs, and Medicare contractors using the SSA telecommunications network. We concluded that security weaknesses existed and to help correct these weaknesses we made nine recommendations. To determine whether SSA had implemented our recommendations, we were asked to respond to the following question:

"Specifically, what GAO recommendations made in the June 5, 1978 report are in the process of actually being implemented? By this we mean what actions are being taken. Please provide appropriate documentation of actual implementation, as SSA oral assurances are unacceptable."

Because our 1978 report included offices under the direction of SSA (district, branch, teleservice centers, program service centers, and DDSs) and HCFA (contractors), we are commenting on various actions taken by each agency. During our earlier review, we briefed the Commissioner of Social Security (December 1976) on security weaknesses we had noted. As a result, SSA began to revise the Systems Security handbook, setting forth guidelines for improving security over beneficiary records in offices under its direction (a completely revised handbook was distributed in June 1978). About the same time, HCFA issued standards to contractors. Both of these documents contain similar instructions designed to correct security weaknesses that we had identified. There are three areas covered by these instructions--(1) administrative safeguards, (2) physical safeguards, and (3) technical safeguards. Each of these documents generally cover the following areas for security:

Administrative safeguards

- Provide security awareness training for employees.
- Develop and maintain a documented security profile which includes a copy of the organization's security policies and procedures.
- Provide for separation of responsibilities in such a way that a system cannot be defrauded by a single individual.

Physical safeguards

- Provide for building security during normal working hours to restrict access to claims processing work areas and data processing operations and establish controls over the use and the storage of personal beneficiary information.
- Provide for building security during nonworking hours to restrict access to all work areas and personal beneficiary data.
- Provide for controls over (1) the physical movement of personal data in hard copy or machine-readable form, (2) the storage of personal data, and (3) changes made to beneficiary data.

Technical safeguards

- Maintain adequate controls during the development, testing, and implementation of new computer programs or program modifications to minimize the risk of improperly modifying personal data in automated files.
- All stored data in automated systems must be controlled to prevent unauthorized usage or compromise of data bases containing personal information.
- Data transmission devices and teleprocessing equipment must be protected from unauthorized usage and sabotage.
- Passwords, if used on automated systems must (1) be changed periodically, (2) be removed from the main memory in computers after they are internally verified to prevent them from being output accidentally by the system, and (3) not be displayed by computer terminals or printers without over-scoring to make them illegible.
- Modifications to existing computer systems must be documented and a statement regarding the impacts of changes on privacy must be included as part of the documentation.

Both documents further require that each contractor/office have a system security coordinator to be responsible for implementing and maintaining the following nine-step structured action plan for Systems Security:

- Determine data processing system security required and review and document this effort annually.

- Create a positive management atmosphere for security through formal and informal training programs, by using posters and reminders, and through informal effectiveness reviews by management.
- Organize for security so that selected employees are accountable for implementation and maintenance of segments of the security program.
- Perform a risk analysis on security.
- Establish and maintain a budget for security.
- Develop a security implementation plan.
- Create a positive operational atmosphere regarding security matters among management officials and employees.
- Conduct security audits periodically.
- Apply corrective action once audits have been completed.

These documents are designed to improve security over beneficiary records and set forth instructions to do so. To determine how these security instructions were working, we examined records of security reviews of 18 SSA offices, visited 10 contractors processing Medicare claims, and contacted 13 DDSs.

MEDICARE CONTRACTORS HAVE MADE SOME
IMPROVEMENT IN SECURITY OVER BENEFICIARY
RECORDS SINCE HCFA ISSUED STANDARDS

Security standards that HCFA issued, requested that contractors assess their existing security procedures and determine whether they were in compliance with the HCFA standards and identify areas needing improvements. Contractors were required to obtain waivers from HCFA for any security standards with which they could not comply. A HCFA official stated that as of September 1981, 99 percent of the contractors/subcontractors have completed their assessments.

During our visits, we found that contractors had developed programs and procedures to improve the security of beneficiary records in accordance with HCFA standards. For example, documentation examined demonstrated that one contractor (1) developed a structured action plan for security, (2) developed and presented security training programs for all of its employees, (3) separated duties and responsibilities of some of its employees so that no one employee had complete control over cases being processed, (4) started controlling visitors at its field installations, and (5) assigned accountability for security to selected employees. Another contractor assessed its security practices and appointed security

officers, developed action plans for improving security for personal beneficiary information, developed and presented training on security for all employees handling Medicare data, and started controlling visitors more closely than before the HCFA standards.

ALTHOUGH SSA SAID IT IMPROVED SECURITY MEASURES, ADHERENCE TO ITS ISSUED SECURITY GUIDELINES IS NOT CONSISTENT

The SSA Systems Security handbook contains guidelines for field offices to follow to improve the safeguards over beneficiary records. There are over 1,300 SSA offices as well as the DDS. SSA in replying to Representative Rose's questions stated that it had taken many steps to protect beneficiary records. Further, it stated that each of these offices had been instructed on how to use the handbook which has been distributed to all of these offices.

To evaluate SSA's response, we examined the System Security handbook, reviewed a sample of security audit reports prepared by SSA regional offices, and contacted 13 DDSs. We determined that most offices now have security officers, locate printers in locked rooms, document contingency plans and backup procedures, and train employees in security awareness.

We, however, did note that there were offices that did not always follow the guidelines, as shown below. Some offices did not

- follow the clean desk policy suggested in the guidelines,
- have control procedures for beneficiary folders during working hours,
- conduct internal reviews of security,
- change the passwords used to open and close the terminals,
- control keys to the office, and
- use a destructive device when disposing of documents containing beneficiary information before disposal.

SPECIFIC RECOMMENDATIONS AND ACTIONS TAKEN BY SSA

In regard to our recommendations, SSA agreed that as of September 1981, two of our nine recommendations have been implemented and SSA is continuing to evaluate and study ways in which the remaining seven can be implemented. Following are the recommendations, agency comments, and the present status of the actions planned or being taken by SSA to implement our recommendations.

Recommendation

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

SSA response/actions

SSA stated that limitations on the number of terminals available for field office use and other operational considerations work against restricting open-area terminals to queries only. However, SSA stated that there are a number of other things that can be done to better control access to and improve the security of these terminals. In this regard, SSA has taken certain steps which it feels will improve security. For example:

- SSA conducted a study in 1978, in which it identified specific transactions which were vulnerable to fraud/abuse. For example, in certain situations, terminal operators are able to enter transactions which create an immediate payment to a beneficiary, without identifying the operator. SSA felt this situation could be controlled by using a unique, secret identifier for these transactions. In January 1981, SSA implemented a test in its Atlanta region of the feasibility of restricting employees on the use of terminals. The test required terminal operators to use a unique, secret identifier. A report on the test was issued by the Atlanta region in April 1981. SSA is continuing to evaluate the results of this test and may expand the concept to other critical transactions.
- SSA is planning to replace terminals in the field offices. Specifications for this replacement require that the equipment have the ability to physically lock each terminal. The ability to positively identify the terminal operator is an optional requirement of these specifications.

Status

As of September 1981, SSA is continuing to evaluate alternative methods of implementing our recommendation.

Recommendation

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

SSA response/action

At the time of our June 1978 report, many offices required alterations to secure the printers. In December 1978, the SSA regional commissioners were directed to have all necessary alterations made to locate printers in secured rooms.

At the time of our review, about 300 printers were in unsecured locations, and as of August 1981, about 100 were still unsecured. The reason they are still unsecured is that new office space leases have not been negotiated that include the necessary alterations to secure the printers. SSA has stated that it will continue to pursue this matter until all printers are in secure areas.

Instructions have been issued to data transmission personnel requiring that they monitor and distribute the printed output.

Status

As of September 1981, SSA is continuing to implement the recommendation.

Recommendations

3. Restrict the ability to create records or to access the national data base to only that data necessary for each specific class of office.
4. 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.

SSA response/actions

SSA maintains a security matrix that is supposed to restrict the SSA operating components to a predefined category of data entry transactions. The security matrix restricts SSA's various operating components to a predefined category of data entry transactions for terminals in field offices. Because of operational needs and work missions, some components have broader access capabilities than others. The matrix has undergone analyses and change to update the capabilities needed by each component. Some capabilities are added and others are removed as needs change. The matrix is supposed to restrict SSA operating components to a predefined category of data entry transactions as determined by analyses of the offices' needs. The matrix, however, does not screen out individuals who are not authorized to access or make changes to the central data files.

When we examined the June 1981 matrix, we found that some of the problems identified in our June 1978 report had not been corrected. Teleservice centers which handle telephone contacts with beneficiaries are authorized only to make changes to existing records; however, they have the capability not only to make changes to existing records, but also to create initial claims.

To better relate the ability to create records or make changes to existing records to employee and maintenance personnel duties and responsibilities SSA has developed an identification system that will require a unique and personal identifier for certain data transmission. SSA has assigned specific employees using a terminal, a unique personal identification number (PIN). PIN is related to the employees' duties and responsibilities. Most employees using terminals in SSA offices, DDSs, and contractors offices need to be able to enter transactions or to query data files on beneficiaries. Each time an employee enters his or her PIN along with the transaction, the system will identify the person entering the transaction.

In addition, SSA has tested an identification system in its Atlanta region. This system is called the log-on/log-off procedure. The program's objective is to (1) restrict the entry of data traffic to authorized personnel only and (2) provide a mechanism whereby effective audit trails may be implemented and maintained. These objectives will be achieved by using this system in conjunction with the PIN and a password. This system will limit terminal operators to a specific type of data transactions. Through this system, SSA will be able to restrict employees' ability to create or make changes to existing records to only situations which conform to their responsibilities and duties. This system has not yet been put in operation on a nationwide basis. The PIN system is being used nationwide on one highly sensitive transaction. This transaction permits the SSA office operator to trigger payments to beneficiaries without a prepayment review. SSA put in the PIN system on this transaction nationwide so that an audit trail was established to assist in identifying the originators of such inputs.

To test the log-on/log-off procedure to determine if it is workable for all telecommunications transactions, SSA has used it in its Atlanta region which involves about 94 SSA offices. SSA plans to use the results of this test to see if it is feasible to develop a system to be used in all offices on the SSA telecommunications system.

Status

As of September 1981, SSA is continuing to evaluate procedures to implement the recommendation.

Recommendation

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

SSA response/action

SSA agreed in principle with the need for an audit trail on input documents. However, SSA does not believe that an audit trail as extensive as we described is prudent. Under established operating procedures, a number of employees will frequently handle a case before authorizing payment. On many short transactions, requiring a personal identifier from each employee in the chain would mean that the audit trail data that SSA must key, transmit, and store would exceed the data itself.

Status

SSA did not fully agree with our recommendation. However, SSA has recognized that there are certain sensitive transactions that may need such an extensive audit trail and has undertaken risk analysis to identify them. As of September 1981, SSA has not implemented the recommendation.

Recommendations

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

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

SSA response/action

SSA stated that in August 1978, additional instructions and guidelines were issued to personnel using terminals and are supposed to operate under the lock/unlock procedures that require:

- Detailed information on the lock/unlock system be provided only to the manager, the director of each operating component, or the designated security officer.
- The manager or director of each operating component (or the security officer) to specify the lock code and provide the code only to persons who absolutely need to know it to fulfill their assigned duties.

--All terminals be locked at the close of each working day. The manager or director of each operating component to be responsible for assuring that this practice is followed uniformly.

In addition, SSA has developed a feature (autolock) which automatically locks terminals 30 minutes (if the terminals remain inactive) after the office's scheduled close of business if they are not locked by the office. When a terminal has been locked by autolock, the office is required to call the regional or component security officer to have the terminal unlocked before it can be used again.

SSA has directed that the lock/unlock password be changed on a weekly basis. Also, SSA is considering developing software to (1) automatically generate replacement lock/unlock passwords for those which are not changed timely and (2) detect and report to regional security officers when passwords are not changed after the specified time period.

Status

Although we noted (see p. 9) that some offices were not complying with the instructions, we believe that SSA's actions satisfy the requirements of these two recommendations. Compliance with the issued instructions is a matter to be dealt with during SSA's security audits.

Recommendation

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

SSA response/action

As noted under SSA action to Recommendation #1, plans for replacement of the terminals include security requirements to improve current security deficiencies. (See discussion under Recommendation #1 on p. 10.)

Status

As of September 1981, SSA is continuing to evaluate the recommendation.

Recommendation

9. That the Secretary of HHS 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.

SSA response/action

SSA has conducted some risk analyses while others are underway or planned. These studies will be analyzed to determine how best to correct the security weaknesses identified in our report and will be used as a basis for the overall security assessment process. On December 1, 1978, SSA stated that it had completed a telecommunication terminal security review in conjunction with the replacement of telecommunication equipment. This review included an indepth study of numerous SSA sites and facilities and presented detailed analyses of many sensitive system applications. SSA said that management actions have been taken to implement many of the recommendations resulting from the review either in whole, in part, or in modified form. Action on other items is awaiting funding.

Three additional studies of risk vulnerabilities were started in 1979. These address privacy and security procedures used by State agencies and contractors to safeguard SSA data and the Claims Automated Processing System.

In June 1981, the SSA Associate Commissioner for Assessment proposed a plan for Systems Security goals and objectives, which is currently being reviewed by SSA management.

Status

SSA is continuing to study and evaluate security problems. Although SSA's present plans should improve security, its management plans indicate this will take about 5 more years to accomplish. (See ch. 3 for more details on what SSA has done and plans to do in security.)

- - - -

Our June 1978 report referred to findings reported by HHS' audits in May and June 1977 which addressed problems in security controls on terminals connected to the SSA telecommunications network. The audits identified security weaknesses that needed immediate corrective action. Many of the weaknesses were similar to those identified and reported by us in June 1978.

During our current review, HHS was performing a followup review to determine what actions had been taken by SSA to correct security problems which it had reported in May and June 1977.

On September 24, 1981, HHS issued a report on its followup work and stated:

"We concluded in our prior reviews that the security controls over the telecommunication system used by the Social Security Administration needed improvement. Adequate controls were not in place to restrict unauthorized terminal access and use. While some corrective actions had been taken on prior recommendations, our follow-up review showed that many system security deficiencies still existed. Even though management had placed increased emphasis on security awareness and implemented new security features, these initiatives were minimally effective and more needs to be done."

In replying to the HHS report findings, SSA stated:

- One of the principle ways SSA is improving its overall security is by developing individual accountability for every transaction entered into SSA systems. Ultimately, we want the ability to trace any transaction to its originator: office, terminal, keyer, authorizer, and reviewer. A variety of measures is being used to attain this goal.
- All of these efforts, however, are constrained by limited resources.
- We are in the process of replacing our terminals and concentrators and will have increased security because the new terminals will all have key locks and the ability to add a number of software safeguards.
- Unfortunately, since SSA is not in a position to concurrently upgrade the central office computers that receive the data, much of the potential increase in capacity will not be realized for some time.
- The audit trail project will be constrained not only by the capacity problems, but also by the limited resources that our Office of Systems has available for software support.
- Lack of programing resources, however, means that we will not be able to install the audit trails as quickly as we would like.

We believe the HHS' audit conclusions, SSA's responses, and our findings are in general agreement.

CHAPTER 3

WHAT SSA HAS DONE AND PLANS TO DO IN SECURITY

Since our briefing of the Commissioner of Social Security in December 1976 and the issuance of our 1978 report, SSA has taken some actions to implement policy, procedures, and organizational changes aimed at increasing security over beneficiary records. SSA has:

- Initiated 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. It 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 in either input or query functions according to their assigned duties and responsibilities.
- Established a Systems Security staff.
- Conducted a study of a computer-related crime vulnerability in the SSI program.
- Held meetings with regional security officers to discuss systems security and privacy matters (latest meeting held in June 1981).
- Recognized the importance of systems security and stated that:

"Although these many projects are underway systems security is still in its developmental stages. As we gain more experience with the functions 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."

As discussed in chapter 2, SSA has taken some actions on our recommendations. Two of the nine recommendations have been implemented and the others are in various stages of completion. Although some actions have been taken, SSA recognizes much needs to be done to implement our recommendations and improve procedures to safeguard its records, as indicated below.

PRESENT SECURITY PROGRAM AND SSA PLANS

In early 1977, the Associate Commissioner for Program Operations--in charge of field offices--established within his

office a permanent Systems Security staff to implement an effective security program. Through this staff the Associate Commissioner could mandate security standards and measures for all field offices. However, in January 1979, the Systems Security staff was reassigned to a new office--Associate Commissioner for Assessment--and now acts in the capacity of (1) developing policies and procedures; (2) coordinating, preparing, and monitoring an SSA Systems Security program; (3) providing direction as necessary; (4) representing SSA to outside agencies; and (5) reviewing security related activities of SSA components.

Under this arrangement the staff will have to rely on the various SSA operating components to implement security improvements and standards and will have to obtain the approval and cooperation from these operating components before any suggested security improvements can be put into effect. In June 1981, the Associate Commissioner for Assessment proposed a plan for Systems Security goals and objectives.

The security goals and objectives cover five specific areas: (1) risk management, (2) physical security, (3) personal security, (4) contingency planning, and (5) Systems Security management support. As of July 1981, the following plan was being reviewed by SSA management.

I. Risk management

A. Risk analysis in operational processes

This process consists of three major steps: (1) risk (vulnerability) assessment, (2) safeguard selection, and (3) safeguard implementation. Some of the activities involved are:

- SSI program.
- Claims automated processing system.
- Manual adjustments, credits, and award process.
- State data exchange system.
- Earnings system.
- Enumeration system.
- Central Office, Electronic Data Processing operations.
- Telecommunications system.

--Electronic Data Processing system design and development process.

B. Monitor risk analysis activity

A tracking and control system will be established to coordinate and track risk management activity (primarily risk analysis and the resulting safeguard implementations).

C. Security implementation

Ensure that all risk analysis findings and recommendations result in positive action--either implementation of a safeguard or further study of the problem. Initiate special studies to examine areas that are particularly vulnerable to program abuse and conduct projects aimed at detecting the existence of program abuse.

D. General program protection safeguards

These constitute a set of common-sense safeguards which will benefit security of all systems.

E. Audit trail improvements

SSA has experimented with a procedure (test) whereby each terminal operator will be assigned a PIN for use in the telecommunications system. Using PIN will allow operators to enter only specific transactions.

The plan calls for expanding the experiment so that eventually a security audit trail record will be established for every transaction that may influence a payment.

II. Physical security

Establish a program for physical security at all SSA installations, based on a set of clear, concise guidelines for each type of facility. Continually enhance physical security through a program of facility "self-audit" supplemented by onsite physical security reviews. This will include (1) establishing new physical security guidelines, (2) enhancing security at SSA facilities, and (3) conducting reviews of physical security at all SSA facilities.

III. Personnel security

The need for an active personnel security program for automatic data processing (ADP) related positions was established in the Office of Management and Budget Circular A-71. This program is to assure that people assigned to positions

of trust are in fact trust-worthy, usually through checks of credit and law enforcement files and background investigations. Directly related to personnel security is an access control system which will automatically notify supervisors to institute or revoke telecommunications access or authorization rights, terminal privilege levels, and change passwords when employees assume or leave the position of trust defined in the personnel security program.

IV. Contingency planning

Establish a plan which will specify a complete course of actions for any type of natural or man-made disaster that might befall SSA central Electronic Data Processing operations.

V. Systems Security Management Support

Undertake action to (1) develop policies and procedures, (2) establish a support structure, and (3) establish a system to assure continued employee awareness and security training.

Many objectives to improve security have been established; however, obstacles within SSA's current management structure may hinder this achievement. Our concerns in this regard are discussed below.

CAN THE PLANNED SECURITY GOALS AND OBJECTIVES BE EFFECTIVELY ACHIEVED UNDER THE PRESENT MANAGEMENT STRUCTURE?

To accomplish the planned goals and objectives, the Systems Security staff will have to obtain the cooperation and agreement of many SSA operating components before specific security measures can be implemented. Present plans indicate that to continue with a security plan and program, resources presently assigned to other SSA operating components will have to be recruited to work on security. Some of the security work to be done in the future will require resources from many different SSA operating components. Depending on the attitude toward security, prevailing workloads and the priorities of the individual SSA operating components, it may be difficult and time consuming to obtain the necessary resources to study various security problems and to reach agreements among other operational components before the security plan and program can reach fruition. In August 1981, the SSA Associate Commissioner for Assessment expressed his concern about this potential problem in a memorandum to the SSA Deputy Commissioner for Programs. He indicated that he had experienced problems in obtaining adequate resources from another SSA operating component in performing risk analyses and as a result, the planned risk analysis completion dates were missed.

CONCLUSIONS

Since we pointed out security weaknesses to the Commissioner of Social Security and recommended corrective actions to better protect beneficiary records to the Secretary of HHS, SSA has taken some actions and has developed plans to implement a security program. SSA also recognizes that more needs to be done to implement our recommendations and create and maintain an aggressive ongoing security program.

The 1979 reassignment of the Systems Security staff placed it in a position of having to obtain the cooperation from several operating components to continue the development and implementation of an adequate security program. This arrangement may very well hinder the implementation of present goals and objectives proposed by the Associate Commissioner for Assessment. We believe that unless there is an office within SSA with the responsibility, capability, and authority for developing, implementing, and managing a security program for the protection of beneficiary records, the achievement of such a program may very well be hindered.

RECOMMENDATIONS TO THE SECRETARY OF HHS

We recommend that the Secretary direct the Commissioner of Social Security to give priority to implementing the June 1978 recommendations.

We also recommend that the Commissioner of Social Security be required to evaluate the current role of the Systems Security staff and the need for an aggressive security program to protect beneficiary records and, if deemed necessary to achieve such a security program, establish an office within SSA with the primary responsibility, capability, and authority for developing, establishing, and maintaining an aggressive ongoing security program for the protection of beneficiary records.

SSA DATA EXCHANGESWITH OTHER FEDERAL AGENCIES

In the original request, we were asked to answer the following questions:

--"Under routine use provisions, [1/] what data on individuals is being given by SSA to other Federal agencies, what use is made of it, is this legally justifiable, and do individuals whose data is being exchanged both know of and consent to such exchanges?"

--"How is the data treated in terms of security and privacy?"

In our initial meetings with your offices, we agreed not to respond to these two questions because another GAO division was reviewing and planning to report on security over Federal data being exchanged among Federal agencies. During a subsequent meeting on March 18, 1981, we were requested to respond to the questions, but only to the extent of highlighting the findings in the report that was prepared by the other GAO division. We agreed to do so.

Our highlights of the report findings and ongoing GAO work related to the reported findings are set forth below.

SSA discloses large amounts of personal beneficiary information to other Federal agencies for use in managing programs. For example, SSA discloses 400,000 records annually to the Railroad Retirement Board to assist it in administering unemployment compensation and pension programs. Personal information on about 8,000 beneficiaries is exchanged annually with the Department of State for use in administering the Social Security Act abroad. These types of disclosures are made by SSA under the routine use provisions of the Privacy Act which do not require prior approval from the beneficiary before the exchange is made.

GAO reviewed the automated systems security in 10 Federal agencies for the Chairman, Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations, and found that security procedures for automated systems processing personal and other sensitive data generally were inadequate.

1/Routine use means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

In a report on that review, 1/ GAO emphasized that Federal agencies

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

GAO recommended that these inadequacies be corrected. GAO reported that the development of comprehensive security programs for automated systems cannot be further postponed because of (1) heavy reliance of agencies on the integrity of computer systems and on data included therein and (2) the increasing potential for fraud, abuse, operational setbacks, and economic losses that could occur from extensive use and reliance on these systems in day-to-day operations. The report pointed out that the Office of Management and Budget issued Circular No. A-71, July 27, 1978--Security of Federal Automated Information Systems--after completion of the review, but before report issuance. This circular requires actions by agency top-level managers which could contribute greatly to correcting many of the computer data security problems addressed in the report. GAO viewed the leadership role by the Office of Management and Budget as vital to maintaining the momentum that Circular A-71 should impart to computer security in Federal agencies. The report expressed concern that agencies might lose sight of the stated purpose of the directive, i.e., that agencies develop and implement computer security programs with a scope to protect personal, proprietary, and other sensitive data.

On December 21, 1979, the Chairman, Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations, requested GAO to follow up on the report recommendations. GAO expects to issue a followup report in late 1981.

1/"Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, Jan. 23, 1979).

OTHER INFORMATION REQUESTED

Chapters 2 and 3 addressed your question about the actions taken by SSA to implement the recommendations in our June 1978 report. Here we answer two other questions as agreed.

To answer the questions, we carefully reviewed SSA's response to Representative Rose, reviewed audit reports issued by the HHS' Office of the Inspector General, and discussed the questions with responsible agency officials. Based on our work, we believe that the information given to Representative Rose by SSA is reasonably accurate. Our answers to your questions, based mainly on what we did, as described above, follow.

Question 1

"At SSA's central complex, ADP maintenance contractors maintain offices and ADP terminals accessing SSA's data banks. Specifically, what access do such people have to SSA's data banks and master beneficiary files and what security measures exist on SSA's part to prevent abuse of such unique access? What abuses, if any, have occurred?"

The SSA central computer facility is located in a secured, guarded area, and ADP maintenance contractors keep offices within this area. Most ADP equipment used to process claims and to store beneficiary records, computer programs, and computer tapes are located here. To be admitted to the area, a person is required to have an authorized identification badge. Once inside, individuals can go anywhere without an escort. SSA does not supervise or monitor maintenance contractors' employees while in the computer complex.

In September 1980, HHS' Office of Inspector General issued a report on physical access to the ADP secure area. The report indicated that security in the area could be improved.

"Security over SSA's data processing facility, computers, and computer record files has not been maximized because unrestricted access to the ADP security area has not been effectively limited. Access badges to the secure area were given out too freely to programmers, food vendors, maintenance staff and others. Badges were not revoked upon retirement or relocation of personnel. Standards specifying the level of access to the secure area and procedures for the guidance of security personnel were not developed. Personnel entering the

secure area were not subject to security investigations, or made aware of the provisions of the Privacy Act of 1974. These noted problems were caused by less than aggressive ADP security management and the lack of coordination of ADP security with SSA's Security Officer."

SSA agreed with the report and stated that it would take corrective action to limit access to the area housing the central computer complex.

There are two contractors who have computer terminals/equipment attached to the central complex. In both cases, SSA has established a control system or procedure designed to prevent abuse or misuse of the information in the computer system.

CONTRACTOR #1

One contractor handles the repairs for terminals located in field offices. When a terminal needs maintenance or repairs, the office transmits a message over the telecommunications network to SSA's computer complex. The contractor's equipment (which is attached to the SSA central computer) accepts the maintenance message from the field office and transmits it to the contractor's office located in Silver Spring, Maryland. The contractor then sends its repair staff to the troubled field office to fix the equipment. SSA stated that procedures ensure that the contractor's equipment is used only for this purpose and not for accessing or altering any data on SSA beneficiaries.

CONTRACTOR #2

Another contractor tests and adjusts system software used by SSA to operate its ADP equipment. When SSA encounters problems with its system software, it contacts the contractor who determines the corrective actions needed to adjust the computer program. To get the corrective information on a timely basis, SSA has installed telecommunications terminals between the contractor's office and its central computer complex. To ensure adequate security, SSA uses a special program for this terminal connection which prevents transmission of any information to the contractor's office. The SSA terminal can only receive information from the contractor that adjusts the computer program to correct the identified problem. To ensure that the terminal is used only to correct identified computer problems, SSA has established the following procedures.

- A. The contractor tells SSA that he or she needs to use the equipment to correct a computer program problem.
- B. An SSA employee gets a key from an SSA safe and unlocks the SSA terminal.

- C. The contractor activates his or her terminal equipment with his or her key.
- D. SSA and the contractor activate the computer program to receive the corrective data.
- E. All data sent to SSA's computer are recorded and subsequently reviewed by the SSA security staff to check for any violation of security.
- F. SSA employees terminate the connection, lock the SSA terminal, and put the key back in the safe.

SSA is not aware of any abuses that may have occurred because of these contractual arrangements.

Question 2

"Have any abuses occurred involving use of dial-up units and their operators, or people with access to them? Please be specific, and include how SSA presently prevents programmers on these units from using phone numbers to gain access to SSA data that is outside his or her particular data bank?"

A "dial-up" unit is a portable terminal. It can be used by connecting it to a regular telephone and can be carried from one office to another. When these units are used to access a computerized data file, the unit operator dials a predetermined telephone number. After making the telephone connection, the unit operator inserts the receiver into the "dial-up" unit. The operator must then enter his or her valid identification code which has been assigned to the individual by an SSA security officer. The operator must also have a valid job and related account number.

In its response to Representative Rose's question, SSA stated that the units are used for (1) mission oriented program data (i.e., processing title II disability claims, managing basic records supporting social security programs, and processing claims for benefits filed by persons in foreign countries) and (2) accessing the management information system. It further stated that:

- On the program data (mission oriented program data), all dial-up connections to computers serving these data banks are restricted to calls made from within SSA's headquarters.
- On the management information system, SSA has installed a terminal security system. Anyone desiring access to the management information system must provide a valid identification code. This code is assigned to individuals by

the security officer only after receiving formal authorization from his or her Division Director. To access a file, the correct code, unique to that individual, and a valid job and associated account number must be entered into the terminal.

SSA is not aware of any abuses that may have occurred.

(105064)









AN EQUAL OPPORTUNITY EMPLOYER

**UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548**

**OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300**

**POSTAGE AND FEES PAID
U. S. GENERAL ACCOUNTING OFFICE**



THIRD CLASS