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

HUMAN RESOURCES
DIVISION

February 21, 1978

B-164031(4)

Mr. Donald I. Wortman
Acting Commissioner of Social Security
Department of Health, Education,
and Welfare

Dear Mr. Wortman:

Although the Social Security Administration has recently spent about $500,000 to install a new security system for its computer operation, the central computer facility is still not secure. Unauthorized personnel have access to the computer room and tape vault. Magnetic tapes, disk packs, and other property can be removed without proper authorization, and blank and valid Social Security and Medicare cards can be taken from the central computer facility without question. Adequate security procedures have not been established, and Social Security has not made an in-depth study of its security needs with respect to the central computer facility.

Acquiring the new security system was a step in the right direction, and with some modifications and the development of adequate procedures, it should prove to be an effective way of preventing unauthorized access to and exits from the central computer facility. However, there is another potentital problem that must be addressed--preventing the fraudulent and malicious acts of persons who work inside the central computer facility. Considering the overall impact Social Security has on millions of Americans, and the results which would occur if its central computer facility's operations were interrupted, we believe that more effective controls and security procedures must be established to protect both Social Security records and property, and the privacy of the American people.

Our observations were made between January 23 and February 3, 1978, as part of our "Review of Internal Controls and Performance of the Supplemental Security Income System." Our findings as well as recommendations for improving the security of your central computer facility were reported to members of your staff on February 10, 1978. A summary of our findings and recommendations are included below.

HRD-78-73
(105013)

NEED TO PREVENT UNAUTHORIZED ACCESS TO AND EXIT FROM THE CENTRAL COMPUTER FACILITY

Unauthorized personnel can easily enter and exit the central computer facility in several ways. First of all, the central computer facility's turnstiles allow movement in both directions once they have been activated by a security badge. Thus several people can enter and exit from a single admission authorization. Since the security guards are not always positioned in direct view of the turnstiles, these unauthorized entrances and exits can go undetected. We demonstrated this by admitting two GAO auditors from a single authorization without the awareness of security guards.

A second way to gain access involves the use of temporary badges. Several of these valid badges can be obtained by an authorized individual and distributed to nonauthorized personnel. Personal identifiers such as social security number, name, and organization are obtained when the badge is issued; however, these identifiers are not used by the automated security system to make sure that only one temporary badge is valid for an authorized person at any point in time. During our observations, we admitted a nonauthorized GAO auditor into the central computer facility. Even with permanent authorization badges with employee pictures, security guards seldom match the person with the picture on the badge. Thus nonauthorized admittance to the central computer could be made if an authorized employee permits it.

Once inside the central computer facility, unauthorized exits can be made through the emergency exits without alarming security guards. These emergency exits are wired with electromagnetic connectors which when separated, set off an alarm. By removing the two screws at the bottom of the connectors, the doors can easily be opened without interrupting the circuit. Unauthorized personnel can thus exit and enter the central computer facility once these doors are opened. During our observations, a GAO auditor took Social Security property through one of the opened emergency doors without the security guards' awareness.

RECOMMENDATIONS

To avoid unauthorized access to and exits from the central computer facility, we recommend that:

--Security guards be positioned in full view of the turnstiles, and that they be required to verify the pictures on the authorization badge with the person using it.

--The security system be modified to allow only one temporary authorization badge to be valid for a person at any given time.

--Emergency exit wiring and connectors be secured to prohibit tampering and thus prevent unauthorized entrances and exits by personnel and property.

MORE CONTROL IS NEEDED OVER MAGNETIC TAPES AND DISK PACKS

Magnetic tapes and disk packs can be removed from the central computer facility without proper authorization because effective control procedures have not been established. Currently, before a magnetic tape can be removed from the central computer facility, a tape dispatch pass is supposed to be obtained from Tape Library Control Section personnel and presented to security guards upon exiting. We were able to remove tapes without tape dispatch passes because security guards did not check notebooks, lunch containers, and brief cases for Social Security property. Furthermore, Tape Library Control Section personnel do not control tape dispatch passes in their possession. We were able to remove 10 tape dispatch passes, and take tapes out of the central computer facility using these passes. Finally, neither Tape Library Control Section personnel nor security guards verify the actual number of tapes which are to be removed from the central computer facility with those actually taken out. From an authorization for a single reel of tape, we were able to remove an entire cart of 38 tapes--two segments of the Supplemental Security Income master file--from the central computer facility. Additionally, with respect to magnetic disk packs only certain individuals have authorization to remove them from the central computer facility. However, we were able to remove a magnetic disk pack without security guard action even though we had not been authorized to do so.

RECOMMENDATIONS

To improve controls over magnetic tapes and disk packs, we recommend that:

--The use of the tape dispatch pass be discontinued, and in its place a transmittal sheet be established to show authorization for removal of tapes and disks and that both the Tape Library Control Section and security guards be required to reconcile the number of tapes by serial number.

--Security guards be reminded of the need to search notebooks, lunch containers, and brief cases of people entering and leaving the central computer facility.

MORE CONTROL IS NEEDED OVER SOCIAL SECURITY AND MEDICARE CARDS

Blank and valid Social Security and Medicare cards are not controlled within the central computer facility and therefore, can be fraudulently removed. During our observations, we found that blank Social Security and Medicare cards were readily accessible at various locations within the central computer facility. We also found thousands of both types of these cards--with valid names and account numbers--which had been discarded because a few had been misprinted. We were able to remove both blank and valid cards from the central computer facility through both the security gates and emergency exits.

RECOMMENDATIONS

In order to provide more control over these identification cards, we recommend that;

--Supplies of blank Social Security and Medicare cards be secured within the central computer facility.

--Effective procedures be established to ensure that nonissuable printed cards be properly destroyed.

--All identification cards be controlled and accounted for as they are used.

NEED FOR A COMPREHENSIVE APPROACH TO SECURING THE CENTRAL COMPUTER FACILITY

Social Security has not developed a comprehensive approach to securing the central computer facility, and no formal in-depth study detailing security requirements and ways to meet

them has ever been made. In July 1976, at the request of Social Security, the MITRE Corporation made "A Preliminary Evaluation of the Physical Security Requirements of the Social Security Administration Data Processing Center." MITRE pointed out that most of Social Security's physical security measures have been implemented on a piece-meal basis. We agree with this finding and believe that the new automated security system is the latest example of this practice. No in-depth risk-analysis has been performed to determine what security procedures should be established, and furthermore, no overall structured approach has been developed for securing the central computer facility.

Social Security's main approach has been to protect itself from unauthorized personnel having access to the central computer facility. However, it has not addressed another potential problem--preventing fraudulent and malicious acts of persons who work inside the computer room. All of the unauthorized acts which we performed during our observations could have just as easily been performed by persons who normally work in the computer room. Most persons having access to the computer room are not given a background investigation, and some of them are not even employed by Social Security.

RECOMMENDATIONS

To improve Social Security's overall security procedures, we recommend that:

--A complete, formal risk-analysis be performed to determine what security procedures need to be established for the central computer facility.

--After the risk-analysis, a detailed structured approach be established for security of the central computer facility.

--At a minimum, background investigations be performed on all employees who work within the central computer facility, including personnel not employed by Social Security.

Please advise us of the actions you propose to take concerning our recommendations.

Sincerely yours,

Franklin A. Curtis

Franklin A. Curtis
Associate Director