

DOCUMENT RESUME

07053 - [B2447495]

[Physical Security Deficiencies at Railroad Retirement Board Headquarters]. HRD-78-162; B-164031(4). August 29, 1978. 4 pp. + enclosure (4 pp.).

Report to William P. Adams, Chairman, Railroad Retirement Board; by Lorton E. Henig (for Gregory J. Ahart, Director, Human Resources Div.).

Issue Area: Federal Information: Implementing the Privacy Act of 1974 (1401); Federally Sponsored or Assisted Income Security Programs: Payment Processes, Procedures, and Systems (1309).

Contact: Human Resources Div.

Budget Function: Income Security: General Retirement and Disability Insurance (601); Income Security: Unemployment Insurance (603); General Government: General Property and Records Management (804).

Congressional Relevance: House Committee on Interstate and Foreign Commerce; Senate Committee on Human Resources.

Authority: Privacy Act of 1974 (P.L. 93-579). P.L. 89-554. =41
C.F.R. 101. OMB Circular A-71. OMB Circular A-108.

A recent GAO report included recommendations for correcting serious physical security deficiencies at the Railroad Retirement Board's Chicago headquarters. Reporting of the findings was delayed until the Board had a reasonable opportunity to take initial corrective actions. Photo identification badges have been issued to employees and are being checked by security guards stationed at building entrances. The Board has begun installing a magnetic key entry system to restrict access to the computer area. Although these measures should reduce access, the Board must do more to insure the physical security and confidentiality of clients' railroad earnings and benefit claims records. The Board should formally assess physical security of its headquarters facilities and develop a comprehensive, coordinated physical security plan which would include manual as well as automated record systems. The Board should consider obtaining the assistance of an outside consultant to perform this work. The Board should also implement the interim procedures suggested in the summary of observations to further increase physical security while the formal physical security assessment is being performed. (RRS)



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

HUMAN RESOURCES
DIVISION

B-164031(4)

August 29, 1978

The Honorable William P. Adams
Chairman, Railroad Retirement Board

Dear Mr. Adams:

During recent months we have met with you and the other Board members and have discussed serious physical security deficiencies we noted at the Railroad Retirement Board's Chicago headquarters. On June 2, 1978, we provided you with the enclosed summary of observations containing the details of our findings and suggestions for correcting the deficiencies noted, as well as selected GAO reports and National Bureau of Standards guidelines on computer security. At that time we agreed--in the best interests of the Board, its employees, and its claimants--to defer formal reporting of our findings until the Board had a reasonable opportunity to take initial corrective actions. In this regard, you assured us that the most serious deficiency--uncontrolled building access--would be corrected by July 1, 1978.

On July 5 and July 7, 1978, we assessed the steps taken by the Board to improve physical security at its headquarters facility. We noted that photo identification badges have been issued to employees and were being checked by the security guards stationed at building entrances. We also noted that the Board had begun installing the magnetic key entry system on computer room entrances, as planned, to restrict access to the computer area. Although these measures should reduce the threats to continuity of Board operations posed by overt destructive acts of potential intruders, we believe the Board must do more to insure the physical security and confidentiality of clients' railroad earnings and benefit claims records. By implementing the interim and long-term measures we suggested in our summary of observations, the Board will more fully comply with the physical security provisions of the Privacy Act of 1974, as discussed below.

HRD-78-162
(105034)

BOARD COMPLIANCE WITH PHYSICAL SECURITY
PROVISIONS OF THE PRIVACY ACT

One of the purposes of the Privacy Act of 1974 (Public Law 93-579 approved December 31, 1974) is to provide certain safeguards to individuals against invasion of personal privacy by requiring Federal agencies to establish rules and procedures for maintaining and protecting personal data in agency records. Provisions of the act require that agencies establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records. The act further requires each agency maintaining a system of records on individuals to publish annually in the Federal Register a notice of the existence and character of records systems. Such notice is to describe, in general terms, what measures (e.g., physical security, personnel screening) have been taken to prevent unauthorized disclosure of records and what categories of individuals within the agency have access.

The Board, in publishing its Federal Register notices and reporting to the Congress on privacy issues, has cited building security and restricted access to the computer facility and files as primary physical safeguards established for many of its records systems. As discussed in our summary of observations, however, we determined that in practice these physical safeguards had not been established at Board headquarters. For example, access to the headquarters building in general, and to the computer area in particular, was not adequately restricted. In addition, microfilm, microfiche and hardcopy records containing detailed personal information on railroad workers were not maintained in locked cabinets, locked rooms or controlled areas restricted to authorized personnel.

By failing to physically secure records containing personal data on railroad workers, the agency has jeopardized the privacy of these individuals and therefore has not complied with the physical security provisions of the Privacy Act. The Board's recent action to secure the headquarters building is a step toward compliance, in our view, but must be supplemented by additional agency actions to attain the degree of physical security required to insure the confidentiality of such personal data.

Our current review was directed only at the Board's compliance with the physical security requirements of the Privacy Act. Office of Management and Budget Circulars

A-71 and A-108 and related directives provide guidelines for establishing administrative and technical as well as physical safeguards as required by the act to insure the confidentiality of records and systems processing personal data. We plan to review and report on the Board's compliance with these additional requirements in the next few months.

RECOMMENDATIONS

We recommend that the Board formally assess the physical security of its headquarters facilities and develop a comprehensive, coordinated physical security plan. This plan should take into account the physical security needs at Board headquarters as well as field office locations and should include manual as well as automated record systems. We believe the Board should consider obtaining the assistance of an outside consultant in performing this work.

We also recommend that the Board implement the additional interim procedures which we suggested in our summary of observations to further increase physical security at Board headquarters while the formal physical security assessment is being performed.

- - - -

For your information and use in considering our recommendations, we are enclosing a copy of our report to the Congress entitled "Procedures to Safeguard Social Security Beneficiary Records Can and Should be Improved" (HRD-78-116, dated June 5, 1978).

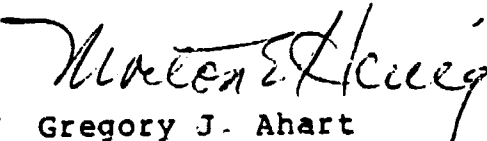
As you know, section 236 of the Legislative Reorganization Act of 1970 requires the head of a Federal agency to submit a written statement on actions taken on our recommendations to the House Committee on Government Operations and the Senate Committee on Governmental Affairs not later than 60 days after the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of the report. We would appreciate receiving copies of these statements.

We are sending copies of this letter to the Chairmen of the House Committee on Government Operations and its Subcommittee on Government Information and Individual Rights; Senate Committee on Governmental Affairs and its

Subcommittee on Intergovernmental Relations; House Committee on Appropriations, Subcommittee on Labor-Health, Education and Welfare; Senate Committee on Appropriations, Subcommittee on Labor, Health, Education, and Welfare; House Committee on Interstate and Foreign Commerce; and the Senate Committee on Human Resources. We are also sending copies to the Director, Office of Management and Budget.

We appreciate the cooperation and assistance provided by Board personnel during our work.

Sincerely yours,


Gregory J. Ahart
Director

Enclosures - 2

SUMMARY OF GAO OBSERVATIONS OF PHYSICAL SECURITY
DEFICIENCIES AT RAILROAD RETIREMENT BOARD HEADQUARTERS
AND SUGGESTIONS FOR IMPROVEMENT

Physical security at the Railroad Retirement Board's Chicago headquarters, especially in its computer facility, is seriously deficient. On normal business days, virtually anyone can enter the building and move about freely. This uncontrolled access poses a threat to the security and confidentiality of valuable individual railroad earnings and benefit claims records--which could be altered, misused, removed, or destroyed--and to the computer area, where only the alertness of the operating staff is relied upon to prevent serious damage to equipment or disruption of operations.

A comprehensive approach to physical security is needed to solve these problems. So far, however, plans for improving security at Board headquarters have been piecemeal and ignore the principal problem of uncontrolled access to the building during normal business hours. Consequently, we believe the Board will be unable to take full advantage of planned improvements that could be useful in establishing an effective physical security system.

RECORDS OF RAILROAD EARNINGS AND BENEFIT
CLAIMS NOT ADEQUATELY SAFEGUARDED

Public Law 89-554 authorizes heads of departments and agencies to prescribe regulations for the custody and preservation of their records, papers, and property. In this regard, each agency maintaining a system of records should provide appropriate safeguards to insure the security of its data. The physical safeguards established at the Board's headquarters, however, are inadequate to insure the security and confidentiality of valuable railroad earnings and benefit claims records. During normal business hours, anyone can enter the building and proceed unimpeded to any of the 12 floors. On most floors, an intruder would find railroad earnings records or benefit claims records in unlocked file cabinets or lying out in the open. These records, which contain valuable personal information needed to support claimant eligibility and benefit payment calculations, could easily be altered, misused, removed, or destroyed, impeding the agency's ability to carry out its primary responsibility--making timely and correct benefit payments to eligible railroad workers.

Opportunities for malicious acts at Board headquarters have been exploited, as evidenced by minor vandalism in the building. According to Board officials, such acts have not been directed at records. Such occurrences, however, clearly demonstrate that destructive persons have been present in the building. Thus, in our view, it is certainly possible that the confidentiality of records may have been breached.

UNCONTROLLED ACCESS TO COMPUTER FACILITY

The lack of adequate physical safeguards in the building poses acute security problems for the area that houses the computer equipment and the tape library. Although Federal Property Management Regulations (41 CFR 101-32.704-4) require Federal agencies to restrict access to computer areas only to essential authorized personnel, we found that anyone can enter the computer area at Board headquarters (through any of four unlocked and unguarded doors) and, in only a few minutes could do extensive damage, disrupting activities for days. Opportunities for tampering or sabotage abound, primarily because Board officials have not (1) designated which employees are authorized to enter the computer area, as required by 41 CFR 101-32.704-4. or (2) routinely required justification for entry.

While visiting the computer facility, we observed a steady flow of persons--some carrying magnetic tapes--entering and leaving unchallenged. We recalled seeing a few of these individuals in the computer programming section, located on the same floor. Allowing programmers in the computer operations area violates one of the basic rules of internal security for automatic data processing facilities.

PLANS TO STRENGTHEN PHYSICAL SECURITY ARE INSUFFICIENT

The Board is planning to strengthen physical security by installing (1) a magnetic key entry system for the main entrances to the building and to the computer room, (2) lockable desks in working areas, and (3) a fireproof wall separating the tape library from the computer facility. Although these measures should enhance physical security, we noted that the magnetic key system will not be used during normal business hours at building entrances; thus,

anyone could still enter the building during these hours and proceed unchallenged to areas where records are kept. Further, the continued ease of entry to the computer area would still place most of the burden of preventing unauthorized entry on the operating staff.

We understand that an overall assessment of Board headquarters security requirements, including a computer security risk and cost analysis, has never been performed. Thus, in our view, the improvements planned by the Board cannot be considered a comprehensive approach to solving the Board's security problems.

SUGGESTIONS FOR IMPROVEMENT

The Board should formally assess the physical security requirements of its headquarters facilities to provide a basis for developing a comprehensive and coordinated physical security plan. In this regard, one of the first actions taken should be the performance of a computer security risk and cost analysis, as provided for under National Bureau of Standards guidelines.

Until these analyses are completed and permanent remedial measures adopted, the Board should immediately implement interim procedures for better securing its headquarters facilities. Because of the practical problems of securing the extensive work, filing, and computer areas (for example, files are distributed throughout the 12 floors), the keystone of such interim procedures should be control over access to the building. Accordingly, the Board should immediately require positive identification of all persons entering the building. Although effective control over access to the building should reduce the security risks to the work, filing, and computer areas, we suggest that the Board also consider:

- physically restricting access to the computer area, essentially the third floor;
- requiring separate, special identification for access to this area, especially the computer room and tape library;
- instituting security patrols within the building to discourage and detect suspicious activities;

--installing exit-only doors on stairways and secondary doorways to main hallways; and

--locking file cabinets or relocating them to restricted-access areas.

Because certain physical security deficiencies at Board headquarters are similar to those we recently identified at the Social Security Administration's headquarters computer facility, we are providing the Board with copies of our February 21, 1978, letter report to that agency and Social Security's April 25, 1978, response detailing its actions--taken and planned--to improve physical security. In considering our suggestions for improving computer security, the Board should also refer to the following publications:

--Comptroller General's Report to the Congress (FGMSD-76-40 dated May 10, 1976) entitled "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities;"

--National Bureau of Standards' Federal Information Processing Standards Publication 41, dated May 30, 1975, entitled "Computer Security Guidelines for Implementing the Privacy Act of 1974;" and

--National Bureau of Standards' Federal Information Processing Standards Publication 31, dated June 1974, entitled "Guidelines for Automatic Data Processing Physical Security and Risk Management."