**Management Information Report**
**Weaknesses in RRB Controls for Protecting Social Security Numbers**
**Report No. 02-05, February 13, 2002**

## INTRODUCTION

This Management Information Report presents serious control weaknesses related to the protection of Social Security Numbers (SSN) and other sensitive information. This situation was noted during the initial stage of an Office of Inspector General (OIG) review of the Railroad Retirement Board's (RRB) Controls Over the Access, Disclosure and Use of SSNs by Third Parties. Due to the sensitive nature of data that has been left unsecured and subject to unauthorized disclosure, this situation is being brought to the RRB's attention for immediate corrective action.

## BACKGROUND

The RRB is an independent agency in the executive branch of the Federal government. The RRB's primary function is to administer comprehensive retirement-survivor and unemployment-sickness benefit programs for the nation's railroad workers and their families. These benefits are provided under the Railroad Retirement Act (RRA) and the Railroad Unemployment Insurance Act (RUIA).

During fiscal year 2000, the RRB paid retirement-survivor benefits to approximately 724,000 beneficiaries. The RRB also paid unemployment and sickness benefits to 35,000 individuals qualifying under the RUIA.

Due to concerns related to perceived widespread sharing of personal information and occurrences of identity theft, Congress asked GAO to study how and to what extent Federal, state and local government agencies use individuals' SSNs and how these entities safeguard records or documents containing those SSNs.

The expanded use of the SSN as a national identifier provides a tempting motive for many unscrupulous individuals to acquire a SSN and use it for illegal purposes. While no one can fully prevent SSN misuse as currently administered, Federal agencies have a responsibility to limit the risk of unauthorized disclosure of SSN information. To that end, the Chairman of the House Ways and Means Subcommittee on Social Security asked the Social Security Administration (SSA) OIG and the President's Council on Integrity and Efficiency (PCIE) to look across government at the way Federal agencies disseminate and control the SSN.

As a result of this request, the PCIE is coordinating reviews of controls over the access, disclosure and use of SSNs by several agencies. Our office is participating in this joint project and has opened an audit at the RRB. The audit is in its initial stages and this report presents the results of only the initial security testing.

## OBJECTIVE, SCOPE AND METHODOLOGY

The objective of the OIG's audit is to assess the RRB's controls over the access, disclosure, and use of SSN information by third parties.

The initial testing included security checks to determine if RRB employees are creating a risk for unauthorized disclosures by discarding documents containing SSNs and other sensitive data in trash cans in their work areas or in trash containers in the elevator hallways. The auditors also looked for RRB documents containing SSNs left unattended in the elevator hallways.

OIG auditors performed the security checks by visiting the elevator lobby areas and associated hallways on each floor of the RRB's headquarters building in Chicago, Illinois and inspecting documents in storage containers, trash containers and trash bags. The security checks were performed between 3:00 p.m. and 4:00 p.m. and again between 4:30 p.m. and 5:30 p.m. on January 24, 2002.

## RESULTS OF REVIEW

Security tests reflect that the RRB is not adequately protecting SSNs and other sensitive information from unauthorized disclosures. Documents containing SSNs and other sensitive information were observed in storage containers, unlocked trash containers and in trash bags located in the elevator lobbies on seven different floors of the building. Attachment A identifies the specific floors where these documents were observed. The following paragraphs provide additional information on this situation.

Several storage containers (boxes and tubs) containing hundreds, or thousands, of RRB documents including claim folders with the names and SSNs of RRB customers were left unattended in the elevator lobby areas of the RRB headquarters building. These documents were discovered on four different floors of the building (3rd, 5th, 7th and 11th floors).

RRB employees' also discarded documents containing names, addresses, SSNs, and/or dates of birth in trash containers in the elevator lobby areas. These documents were discovered on three different floors of the building (4th, 5th and 11th floors). In some instances, locked trash containers were available and labeled "SHREDDING CONTAINER for Privacy Act Materials ONLY." One of these containers had a padlock but it was left unlocked. Documents containing SSNs and other sensitive data were in this container. Containers on other floors either did not contain locks or were not designed to be locked. One of the containers, which was not designed to be locked, was located on the fourth floor. This container held numerous medical records, which included names, addresses, SSNs, dates of birth, and other medical information that could be considered very private information.

We observed 17 lockable containers on the twelfth floor of the RRB building that were not being used.

It also appears that RRB employees are discarding documents with SSNs in the trashcans in their work areas. Documents containing SSNs were found in trash bags in the lobbies next to the freight elevators. These documents were discovered on three different floors of the building (2nd, 6th, and 11th floor). Cleaning personnel collect trash from individual trashcans in the working areas and place it in trash bags, which are put next to the freight elevator for later transportation to the loading dock.

The Privacy Act of 1974 states that the Congress finds the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies. The purpose of the Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to, among other things, disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose and that adequate safeguards are provided to prevent misuse of such information.

Individuals allowed access to the RRB building for a variety of reasons have access to the unsecured documents and trash containing SSNs and other sensitive data. This data could be used for identity theft. The misuse of the SSN has quickly become a national dilemma. The universal use of the SSN has given it a lot of power. The powers to engage in financial transactions, obtain personal information, and create or commandeer identities make it a valuable asset and one that is subject to limitless abuse. For example, the SSA/OIG received 46,840 allegations of SSN misuse in fiscal year 2000 and has also reported instances of SSN misuse by SSA employees.

In addition to the above documents, the RRB discarded a number of plastic cards used to produce building identification (ID) cards. These cards were in a box on the floor of the 12th floor where the RRB had recently issued new building ID cards. On one side, these cards were very similar in appearance to the ID cards issued to RRB employees. The first line on this side of the cards contained the words “Temporary Building Admittance” in red print. The other side of the cards contained the words “U.S. Railroad Retirement Board” and “Groundhog Job Shadow Day” along with a small picture of two groundhogs. Some of the cards were imprinted with individual names. An individual could cover the words “Groundhog Job Shadow Day” and the picture of the two groundhogs with a picture of themselves. The ID card would then be very similar to the employee ID cards and an unauthorized individual would have a good chance of gaining entry to the RRB building. These ID cards could be picked up by RRB employees, cleaning personnel, and employees of contractors working in the building.

## Recommendations

The OIG recommends that the Senior Executive Officer:

- take steps to ensure that RRB employees protect SSNs and other sensitive data against unauthorized disclosures (Recommendation No. 1);

- take immediate steps to secure documents in the elevator lobbies that contain names, SSNs and other sensitive information (Recommendation No. 2);

- take steps to ensure that locked containers are available on each floor of the building for disposition of documents containing sensitive data (Recommendation No. 3); and

- take steps to appropriately secure or properly discard the ID cards located on the 12th floor (Recommendation No. 4).

## Management's Response

The Senior Executive Officer concurred with recommendations #1, #3, and #4, but did not fully agree with recommendation #2. The Senior Executive Office did not agree that the practice of temporarily storing claim files in centrally located bins constitutes an unwarranted security risk. However, the Senior Executive Officer will consider alternative methods of storage in an effort to enhance security without adversely affecting workflows or significantly increasing costs.

## OIG's Comments on Management's Response

The OIG recognizes the RRB's need to keep equipment and personnel costs low. The OIG is however concerned with the practice of leaving claim folders and other documents in the elevator lobbies unsupervised for extended periods of time or overnight. In considering alternative methods of storing the documents being sent to the Federal Records Center or other RRB locations, the RRB should pursue the possibility of storing the documents within the RRB work areas or other secured areas rather than in the elevator lobbies. RRB employees would then be better able to observe and supervise the documents during working hours and able to secure them after working hours. This small change in location should not adversely affect workflow or significantly increase costs.