

**Review of RRB's Controls Over the Access,
Disclosure and Use of SSNs by Third Parties
Report No. 02-11, August 26, 2002**

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) review of the Railroad Retirement Board's (RRB) controls over the access, disclosure and use of Social Security Numbers (SSNs) by third parties.

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 and the Railroad Unemployment Insurance Act. During fiscal year 2001, the RRB paid nearly \$8.4 billion in retirement-survivor benefits to approximately 700,000 beneficiaries.

The Social Security Administration (SSA) created the SSN in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. However, over the years, the SSN has become a "de facto" national identifier used by Federal agencies, state and local governments, and private organizations. Government agencies frequently ask individuals for their SSNs to comply with applicable laws and regulations or to efficiently track and exchange information. A number of laws and regulations also impose limitations on how agencies may use SSNs.

Due to concerns related to perceived widespread sharing of personal information and occurrences of identity theft, the General Accounting Office (GAO) studied 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. As part of the study, GAO sent questionnaires to 18 Federal programs that were likely to routinely collect, maintain, and use individuals' SSNs. The RRB was not selected for the GAO study. Specifically, GAO's questionnaires asked each Federal program to provide information about the following:

- ways in which the program obtains, maintains, and uses individuals' SSNs;
- current practices for providing individuals' SSNs to other organizations, including fees charged; and
- practices for safeguarding records containing SSNs.

GAO's study showed that government agencies are taking steps to safeguard SSNs; however, certain measures that could help protect SSNs are not uniformly in place at any level of government. First, when requesting SSNs, government agencies are not consistently providing individuals with information required by Federal law. For

example, agencies are not consistently informing the SSN holders of whether they must provide the SSN to receive benefits or services and how the SSN will be used. Second, although agencies are taking steps to safeguard the SSNs from improper disclosure, the survey identified potential weaknesses in the security of information systems at all levels of government. The reviews also found numerous examples of actions taken to limit the presence of SSNs on documents that are not intended to be public but are nonetheless seen by others.

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, Federal agencies have some responsibility to limit the risk of unauthorized disclosure of SSN information. To that end, the Chairman of the House of Representatives' Ways and Means Subcommittee on Social Security asked 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. Several Federal agencies, including the RRB, participated in this joint project and the PCIE coordinated the review.

The Freedom of Information Act, the Privacy Act of 1974, and the Social Security Act Amendments of 1990 establish the framework for restricting SSN disclosure.¹ Specifically, with regard to collecting SSN information, section 7 of the Privacy Act prohibits any Federal, state or local government entity from conditioning any benefit on SSN disclosure by the individual, unless permitted by Federal law.

With regard to disclosures of SSNs contained in Federal record systems (i.e., records maintained on individuals), the Privacy Act controls the use and disclosure of such personal information, but does not specifically address SSNs. For each record system maintained by an agency, a Privacy Act notice must be published informing, among other things, the routine uses and disclosures of that information, which of course will include the SSN if relevant.

The Information Resources Management Center supports the RRB's Chief Information Officer in fulfilling responsibilities required by the Privacy Act. Administrative Circular IRM-2 describes the RRB's responsibilities under the Privacy Act. The circular also provides the responsibilities for the RRB's Privacy Act Officer under the Privacy Act. These responsibilities include the following:

- to provide guidance, technical assistance, and general oversight for compliance with the Privacy Act;
- to serve as the focal point for RRB Privacy Act activities and as the primary liaison with the Office of Management and Budget, and the Office of Federal Register for Privacy Act Matters;
- to review routine use disclosures, exemptions of systems of records, Privacy Act training, and systems of record notices as required by OMB Circular A-130; and

¹ Freedom of Information Act (5 United States Code § 552), Privacy Act of 1974 (5 United States Code § 552a), and the Social Security Act Amendments of 1990 (42 United States Code § 405(c)(2)(C)(viii).

- to coordinate efforts among the bureaus and offices to furnish records to requestors.

OBJECTIVE, SCOPE AND METHODOLOGY

The objective of this review was to assess the RRB's controls over the access, disclosure and use of SSN information by third parties. Specifically, we determined whether the RRB:

- made legal and informed disclosures of SSNs to third parties;
- had appropriate controls over contractors' access and use of SSNs;
- had appropriate controls over other entities', excluding government entities and contractors, access and use of SSNs; and
- had adequate controls over access to individuals' SSNs maintained in its databases.

In accordance with the PCIE guidelines, the review was limited to RRB controls over the access, disclosure and use of RRB beneficiaries' SSN information by third parties. The review covered calendar year 2001 activities. Some information has been provided for earlier and subsequent years because the RRB reports on a fiscal year basis, and some contracts covered multiple years.

To accomplish the objective, the OIG:

- reviewed applicable laws and regulations;
- reviewed prior audit reports;
- submitted GAO's questionnaire to applicable RRB officials;
- reviewed the RRB's controls over the disclosure of and access to SSN information by third parties;
- judgmentally selected and reviewed disclosures to three Federal agencies, three state agencies, two researchers, two private contractors, a railroad, and six insurance companies for compliance with the Privacy Act, as well as applicable agreements between parties;
- interviewed RRB personnel responsible for controlling SSN disclosure and access; and
- provided examples of additional steps that the agency can take to ensure that it has adequate controls over the use and protection of SSNs.

The review was performed in accordance with generally accepted government auditing standards appropriate for this type of review. The fieldwork was performed at the RRB headquarters office in Chicago, Illinois from January through July 2002.

RESULTS OF REVIEW

The review showed that RRB controls over the access, disclosure and use of SSNs by third parties are generally adequate but improvements can be made. The RRB made legal and informed disclosures of SSNs to Federal and state agencies, contractors,

insurance companies, universities, researchers, and railroads through the administration of the RRA and RUIA programs. Prior to disclosing SSN information, the RRB notified all individuals who applied for benefits that their SSNs may be disclosed.

The RRB also released SSNs of deceased beneficiaries to non-government entities and non-contractors. The RRB's Privacy Act Officer stated that the Privacy Act does not protect death information. Therefore, the RRB did not have any control issues in this area.

The RRB can strengthen some controls over contractors' access and use of SSNs and controls over access to SSNs maintained in the RRB's databases. The following sections of the report provide a detailed discussion of areas where improvements can be made.

SERVICES PROVIDED BY CONTRACTORS

The RRB has some controls over contractors' access and use of SSNs. For example, the RRB included the Privacy Act Notification in contracts or referenced the Privacy Act, conducted inspections of contractors' facilities, and addressed the disposition of SSNs and other identifying information. However, controls can be strengthened.

The RRB's Office of Administration and the Office of Programs indicated that they provided information, including SSNs, to four private contractors who provide services for RRB programs. We reviewed two contracts, Consultative Examinations, Ltd. (CEL) and Commercial Data Centers, Inc. (CDC), and determined that controls over the access and use of SSNs could be improved.

CEL provides medical opinions on approximately 8,000 RRB disability claims per year. The contractor is responsible for the daily pick-up and return of case files from the RRB headquarters and advisory medical opinions to the RRB headquarters within the time frames prescribed in the contract.

The contract provided that CEL would maintain a dedicated suite for only RRB work, the suite would be locked at all times, and cabinets used to store files would be fireproof. CEL's technical proposal called for an inventory control system with an up-to-the-minute status report on each claim file.

The RRB's solicitation urged the agency to inspect the site at which services were to be performed. In addition, the Federal Acquisition Regulation provided that the contracting officer should insert a clause allowing on-site inspections.² The clause states that to the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of government data, the contractor shall afford the government access to the contractor's facilities, operations, documentation, records and databases.

² Federal Acquisition Regulation 52.239.1- Privacy or Security Safeguards.

A previous OIG audit performed in 2001 indicated that CEL did not specify how the contractor would comply with the Privacy Act and contract provisions regarding the privacy, confidentiality, and safety of RRB case files.³ These situations were corrected in calendar year 2001.

The OIG audit also disclosed that the RRB did not inspect the facility after the contract was awarded in October 2000. Because the RRB did not inspect CEL's facility in 2001, the RRB had no assurance that its sensitive documents were protected from unauthorized disclosure. The OIG recommended in its report that the RRB perform periodic unannounced reviews of the contractor's facility.

The RRB performed the unannounced inspection of the CEL facility on March 27, 2002 and found: (1) an unsecured dedicated suite, (2) loss of accountability of case files, and (3) case files stored in a non-fireproof cabinet. The contractor resolved all three issues. The RRB indicated it would conduct periodic reviews of the contractor's facility during calendar year 2002.

The RRB used the other private contractor, CDC, to produce and mass mail 717,823 annual tax statements and approximately 300,000 service and compensation records to RRA beneficiaries in calendar year 2001.

The contract with CDC included appropriate security procedures for safeguarding SSNs including the Privacy Act Notification. The RRB visited the contractor's location to determine the accuracy and timeliness of the tax statements and to review storage locations. The visitation included limited security checks related to document storage and the destruction of documents with printing errors. The inspection did not verify other procedures identified in CDC's Security Plan, such as access control, use of log sheets, issuance and control of magnetic cards, and password control. The RRB's visitation did not cover the other CDC security procedures because the RRB's on-site inspection checklist provided for only limited inspection of security procedures. Without sufficiently inspecting or otherwise evaluating the adequacy of CDC's operations, the RRB cannot be assured that the contractor is safeguarding SSNs and other sensitive information.

Recommendation

The Office of Programs should take steps to evaluate and ensure the adequacy of CDC's procedures for safeguarding SSNs and other sensitive information (Recommendation No. 1).

Management's Response

³ Report No. 02-02, Review of the RRB's Contract with CEL for Medical Consulting Services, dated January 4, 2002.

The Office of Programs concurs with this recommendation. The Office of Programs will take steps to evaluate and ensure the adequacy of CDC's procedures for safeguarding SSNs and other sensitive information. These actions will be completed to coincide with the next production run of the contract with CDC. A complete copy of the response is included as Attachment 1.

ACCESS TO SSNs MAINTAINED IN RRB DATABASES

The RRB has established some controls over access to SSNs maintained in its databases. For example, database users must be authorized by a systems administrator, have a system password, and have access to system information only to the extent needed to perform their jobs. However, controls can be strengthened.

In calendar year 2001, the OIG reviewed information security at the RRB pursuant to the requirements of the Government Information Security Reform Act.⁴ The scope of the review covered information system security at the RRB during May through September 2001. The review disclosed weaknesses in most areas of the RRB's information security program. Significant deficiencies in program management and access controls made the agency's information security program a material weakness in internal control over financial reporting. The OIG made specific recommendations for corrective action. The RRB indicated that they have implemented many of the recommendations. The OIG, however, still considers the agency to have a material weakness related to information security due to inadequacies in access controls and training of key personnel.

In addition, three employees with the Centers for Medicare and Medicaid Services (CMS) had direct access to RRB databases, in calendar year 2001. RRB management identified them as the only individuals, other than RRB employees, with direct access to RRB databases.

The RRB's Bureau of Information Services performs an annual security audit and distributes the report to system owners. The owners then provide feedback on the access needs of the individuals in the report. However, this report lists only RRB employees with access to RRB computer systems.

Appendix III to OMB Circular A-130 requires that Federal agencies implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

If CMS employees were included on this list, the control could be effective in identifying CMS employees who have access to system features that they do not need for the performance of their duties. Unneeded system access could allow unauthorized disclosures of SSNs. During calendar year 2001, the RRB relied on CMS to notify the RRB when access needs change.

⁴ Report No. 02-04, Review of Information Security at the Railroad Retirement Board, dated February 5, 2002.

Recommendation

The Bureau of Information Services should include non-RRB employees in future security reports (Recommendation No. 2).

Management's Response

The Bureau of Information Services concurs with this recommendation. Non-RRB employees who have access to RRB computer systems will be included in the annual security audit. This will take effect October 1, 2002 for the two CMS employees.

REPORT TABLE

Objective #1: To determine whether your agency makes legal and informed disclosures of SSNs to third parties.

<p>A. Does the agency make legal and informed disclosures of SSNs to third parties? <i>If yes, only answer B and then go to Objective 2. If no, answer questions B, C, & D, as appropriate.</i></p>	<p>YES</p>
<p>B. Please provide an example or two of how your agency makes legal and informed disclosures of SSNs to third parties.</p> <p>The Railroad Retirement Board (RRB) provides information that discloses individuals' SSNs to Federal and state agencies, contractors, insurance companies, universities, researchers, and railroads through its administration of the Railroad Retirement Act and Railroad Unemployment Insurance Act.</p> <ul style="list-style-type: none"> ➤ The RRB has state wage matching agreements with all 50 states, the District of Columbia and Puerto Rico. Under the agreements, the RRB provides the states with the SSNs of RRB claimants and beneficiaries. The states return wage or unemployment benefit information to the RRB. This information enables the RRB to identify individuals receiving payments from non-railroad employers, or state unemployment benefits, for days they also claim railroad unemployment or sickness benefits. The matching agreements are also used to monitor the earnings of railroad disability annuitants. ➤ The RRB provides identifying information, including SSNs, to the Department of Veterans Affairs. The RRB has the authority to release information to the Department of Veterans Affairs to determine if claimants are eligible for veteran benefits and if any previous veteran benefits were paid incorrectly. ➤ The RRB also provides information, including individuals' SSNs to contractors. One contractor, Consultative Examinations, Ltd. (CEL), provides medical opinions on approximately 8,000 RRB disability claims per year. The contractor is responsible for the daily pick-up of case files from the RRB headquarters and for the delivery of case files and advisory medical opinions to the RRB headquarters within the time frames prescribed in the contract. 	

Objective #2: To determine whether your agency has appropriate controls over contractor's access and use of SSNs.

<p>A. Does your agency use contractors? <i>If yes, continue to question B. If no, go to Objective #3</i></p>	<p>YES</p>
<p>B. Does your agency have appropriate controls over contractors' access and use of SSNs? <i>If yes, only answer C and go on to Objective #3. If no, answer questions C, D, and E as appropriate.</i></p>	<p>NO</p>
<p>C. Please provide an example or two of how your agency has appropriate controls over contractors' access and use of SSNs.</p> <p>We reviewed two written contracts the RRB had in force during 2001: one with CEL, and the other with Commercial Data Centers, Inc. (CDC). CEL provides medical opinions on approximately 8,000 RRB disability claims per year. The contractor is responsible for the daily pick-up of case files from the RRB headquarters and for the delivery of case files and advisory medical opinions to the RRB headquarters. CDC issues RRB Tax Statements (Form 1099) to beneficiaries who received railroad retirement annuities during the tax year and Certificates of Service Months & Compensation (Form BA-6) to current railroad employees.</p> <p>One contract states that the contractor will ensure the privacy, confidentiality, and safety of the physical and electronic case files while the files are in the possession of the contractor. The other contract provides that information regarding any individual is of a confidential nature and must be handled so that such information does not have any unauthorized use.</p> <p>In addition, both contracts provide for the return of all individual information when it is no longer needed.</p>	

D. Briefly describe the specifics of how your agency fails to have adequate controls over contractors' access and use of SSNs. For example, your agency does not (1) have a MOU or written agreement that outlines how contractor's should use and protect SSNs or (2) monitor contractors' access and use of SSNs.

- The RRB did not perform an on-site inspection of CEL's facility in calendar year 2001. The RRB did perform an unannounced inspection of CEL's facility on March 27, 2002 and found the following: (1) an unsecured dedicated suite, (2) loss of accountability of case files, and (3) case files stored in a non-fireproof cabinet. The contractor resolved all three issues and the RRB indicated it would conduct periodic reviews of the contractor's facility during calendar year 2002.
- The RRB visited the CDC's processing location to determine the accuracy and timeliness of the tax statements and to review storage locations. The visitation included limited security checks related to document storage and the destruction of documents with printing errors. However, the inspection did not verify other procedures identified in CDC's Security Plan, such as: access control, use of log sheets, issuance and control of magnetic cards and password control.

E. List specific steps (you identified) that your agency can take to ensure it has adequate controls over access to SSNs maintained in its databases.

The Office of Programs should take steps to evaluate and ensure the adequacy of CDC's procedures for safeguarding SSNs and other sensitive information.

Objective #3: To determine whether your agency has appropriate controls other entities' (non-government/non-contractor) access and use of SSNs.

<p>A. Does your agency grant other entities (non-government / non-contractor) access and use of SSNs? <i>If yes, continue to question B. If no, go to Objective #4.</i></p>	<p>YES</p>
<p>B. Does your agency have appropriate controls over other entities' (non-government / non-contractor) access and use of SSNs? <i>If yes, only answer C and go on to Objective #4. If no, answer questions C, D, and E as appropriate.</i></p>	<p>N/A</p>
<p>C. Please provide an example or two of how your agency has appropriate controls over other entities' (non-government / non-contractor) access and use of SSNs.</p> <p>The RRB disclosed claimant's identifying information to the following non-government / non-contractor entities during calendar year 2001: Asset Quest, Union Pacific Railroad, and six insurance companies. All of the information provided related to deceased individuals.</p> <p>RRB personnel contact the RRB's Privacy Act Officer and the Bureau of Law for guidance before releasing the information. Since the information disclosed related to deceased individuals only, no controls are necessary. Death information is not protected by the Privacy Act.</p>	

Objective #4: To determine whether your agency has adequate controls over access to individuals' SSNs maintained in its databases.

<p>A. Does your agency grant access to SSNs maintained in its databases to individuals affiliated with other organizations? <i>If yes, continue to question B. If no, you are finished.</i></p>	<p>YES</p>
<p>B. Does your agency have adequate controls over access to SSNs maintained in its databases? <i>If yes, only answer C. If no, answer questions C, D, and E as appropriate.</i></p>	<p>NO</p>
<p>C. Please provide an example or two of the controls your agency has over access to SSNs maintained in its databases.</p> <p>RRB database users must be authorized by a system's administrator, must have a system's password, and can access system information only to the extent needed to perform their jobs.</p>	

D. Briefly describe the specifics of how your agency fails to have adequate controls over access to SSNs maintained in its databases. For example, your agency does not have (1) a MOU or written agreement that outlines how personnel from other organizations should safeguard SSNs or (2) system controls to preclude unauthorized employees from gaining access to SSNs maintained in its databases.

In calendar year 2001, the OIG reviewed information security at the RRB pursuant to the requirements of the Government Information Security Reform Act.⁵ The Scope of the review covered information system security at the RRB during May through September 2001. The review disclosed weaknesses in most areas of the RRB's information security program. Significant deficiencies in program management and access controls made the agency's information security program a material weakness in internal control over financial reporting. The OIG made specific recommendations for corrective action. The RRB indicated that they have implemented many of the recommendations. The OIG, however, still considers the agency to have a material weakness related to information security due to inadequacies in access controls and training of key personnel.

In addition, three employees with the Centers for Medicare and Medicaid Services (CMS) had direct access to RRB databases in calendar year 2001. RRB management identified them as the only individuals, other than RRB employees, with direct access to RRB databases.

The RRB's Bureau of Information Services performs an annual security audit and distributes a report to system owners. The owners then provide feedback as to whether the individuals in the report still need the access provided to them. However, the report lists only RRB employees with access to RRB computer systems.

If CMS employees were included in this report, the control could be effective in identifying CMS employees who have access to system features that they do not need for the performance of their duties. Unneeded system access could allow unauthorized disclosures of SSNs. During calendar year 2001, the RRB relied on CMS to notify the RRB when access needs change.

E. List specific steps (you identified) that your agency can take to ensure it has adequate controls over access to SSNs maintained in its databases.

The RRB should include non-RRB employees in future security reports.

⁵ Report No. 02-04, Review of Information Security at the Railroad Retirement Board, dated February 5, 2002.



UNITED STATES GOVERNMENT


FORM G-115f (1-92)

MEMORANDUM

RAILROAD RETIREMENT BOARD

August 16, 2002

TO: Henrietta B. Shaw
Assistant Inspector General For Audit

FROM: Steven A. Bartholow 
General Counsel/Senior Executive Officer

SUBJECT: Draft Report – Review of the Railroad Retirement Board’s Controls over the Access, Disclosure, and Use of Social Security Numbers by Third Parties

This is in response to your memorandum dated August 2, 2002, whereby you transmitted a copy of the above captioned draft report and requested that we review and comment thereon. You asked for two separate written responses, one addressing the draft report and one addressing the report table. Since the report and recommendations concern the Office of Programs and the Bureau of Information Services, we requested the Director of Programs and the Chief Information Officer to review and comment on the draft report. Attached are their comments.

Thank you for the opportunity to review and comment on the draft report.

Attachment

cc: Director of Programs
Chief Information Officer
Director of Assessment and Training
Chief Division of Information Management

**COMMENTS OF THE OFFICE OF PROGRAMS AND THE
BUREAU OF INFORMATION SERVICES**

Comments on Draft Report

Recommendation No. 1: The Office of Programs concurs with this recommendation. We will take steps to evaluate and ensure the adequacy of CDC's (Commercial Data Centers, Inc.) procedures for safeguarding SSNs (social security numbers) and other sensitive information. Our actions will be completed to coincide with the next production run of our contract with CDC.

Recommendation No. 2: Although this recommendation is not directed to the Office of Programs, we agree that including non-RRB employees in future reports is a good security improvement. We would like to point out that the Office of Programs, during Calendar Year 2002, initiated an annual recertification of CMS (Centers for Medicare and Medicaid Services) staff access needs to certain RRB computer systems. Because of this, we ask that the word "currently" in the last sentence of the narrative for the recommendation be replaced with "during Calendar Year 2001, the period the review covered."

The Chief Information Officer concurs with this recommendation to include non-RRB employees who have access to RRB computer systems in the annual security audit. This will take effect October 1, 2002 for the two Center for Medicare and Medicaid Services employees.

Comments on Report Table

Objective #2E: The Office of Programs concurs. We will take steps to evaluate and ensure the adequacy of CDC's procedures for safeguarding SSNs and other sensitive information. Our actions will be completed to coincide with the next production run of our contract with CDC.

Objective #4D: Although the control specified in 4E is not directed to the Office of Programs, we agree that including non-RRB employees in future reports is a good security improvement. We would like to point out that the Office of Programs, during Calendar Year 2002, initiated an annual recertification of CMS staff access needs to certain RRB computer systems. Because of this, we ask that the word "currently" in the last sentence of 4D be replaced with "during Calendar Year 2001, the period the review covered."

The Chief Information Officer notes that on page 1 of the Report Table, the RRB does not provide SSNs to the VA (Veterans' Administration). The VA sends SSNs to the RRB and the RRB furnishes RRB benefit information for hits. However, the RRB does send SSNs to the Social Security Administration under two matching programs.