governmentattic.org
"Rummaging in the government's attic"

Description of document:	Railroad Retirement Board (RRB) Administrative Circular IRM-2: Management of Information Privacy for Individuals, September 3, 2008
Requested date:	28-October-2016
Released date:	21-November-2016
Posted date:	12-December-2016
Source of document:	Freedom of Information Request Chief FOIA Officer (General Counsel) Railroad Retirement Board 844 North Rush Street Chicago, Illinois 60611-1275

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

UNITED STATES OF AMERICA
RAILROAD RETIREMENT BOARD
844 NORTH RUSH STREET
CHICAGO, ILLINOIS 60611-2092

GENERAL COUNSEL

NOV 21 2016

Re: Freedom of Information Act Request dated October 28, 2016

C. 17-0528

This is in response to your letter dated October 28, 2016, received on November 7, 2016, to the Railroad Retirement Board (hereinafter the Board) wherein you requested "the most recent internal FOIA procedures document."

You made your request pursuant to the Freedom of Information Act.

As you are aware, the Board is an independent agency in the executive branch of the United States Government which is charged with the administration of the Railroad Retirement Act (45 U.S.C. § 231 et seq.) and the Railroad Unemployment Insurance Act (45 U.S.C. § 351 et seq.). The Railroad Retirement Act replaces the Social Security Act with respect to employment in the railroad industry.

Pursuant to your request, please find enclosed a copy of the Board's Administrative Circular IRM-2, *Management of Information Privacy for Individuals* (September 3, 2008). For your information, the September 3, 2008 version is the most recent IRM-2.

I trust that this is responsive to your request.

Appeal Rights.

The regulations of the Railroad Retirement Board provide that you may appeal the denial of the requested information by writing to the Secretary to the Board, Railroad Retirement Board, 844 North Rush Street, Chicago, Illinois 60611-2092, within 20 days following receipt of this letter. A letter of appeal must include reference to, or a copy of, this letter.

Sincerely,

Karl T. Blank
General Counsel

Enclosure

SUBJECT: MANAGEMENT OF INFORMATION PRIVACY FOR INDIVIDUALS

SUBJECT: MANAGEMENT OF INFORMATION PRIVACY FOR INDIVIDUALS

I. Purpose

The purpose of this administrative circular is to delineate responsibilities under the Privacy Act, the Freedom of Information Act; Federal Information Security Management Act (FISMA), E-Government Act of 2002, Railroad Retirement and Unemployment Insurance Acts, Internal Revenue Code, and various OMB, NIST and other Federal guidance concerning the management of information about individuals.

II. Authorities

Board implementing regulations.

Railroad Retirement Act (45 U.S.C. §§ 231 et. seq.), Regulations (20 CFR §§ 200-295)

Railroad Unemployment Insurance Act (45 U.S.C. §§ 351 et. seq.), Regulations (20 CFR §§ 300-350)

Railroad Retirement Tax Act (26 U.S.C. §§ 3201 et. seq.)

Internal Revenue Code (26 U.S.C.§ 6103)

Executive Order 13392, Improving Agency Disclosure of Information

III. Definitions

Access

The right of the subject individual under the Privacy Act to be informed, in response to his or her request, whether a Federal agency maintains any record on him or her, and if it does, to see the record and to have a copy made of it in a form that is understandable to him or her. Subject individuals have access to their records; third parties do not, although records of the subject individual may be disclosed to third parties under certain circumstances. (See *Disclosure*.)

Accounting of disclosure

The requirement that Federal agencies be able to develop and document a listing of all but specific exempted disclosures of records of a subject individual, if requested to do so by the subject individual.

Altered system report

A report required by OMB Circular A-130 to be prepared by agencies whenever they create a new routine use or otherwise substantially alter a Privacy Act system of records. The report is sent to OMB and the Congress.

Authorized third party request

A request made for a record maintained in a Privacy Act system of records by a person who is authorized in writing by the subject individual to see or have a copy of their records. Attorneys who submit power of attorney are authorized third party requesters.

Browsing

Browsing refers to willful, unauthorized inspection of federally-owned information about individuals, in particular tax return information.

Disclosure

The act of revealing information. For the purposes of this circular, disclosure means releasing federally-owned information about an individual—personal information, personally identifiable information, or information in identifiable form—to an entity other than the individual, whether or not the information is maintained in a Privacy Act system of records. Improper disclosure would be a disclosure other than one permitted by the Privacy Act or the Computer Matching and Privacy Protection Act, an applicable routine use in the system of records, a RRB standard disclosure, or one authorized in writing by the individual who is the subject of the record disclosed. A disclosure may also be improper if it is made by a person who is not authorized to access the records (see *Browsing*).

Federal Tax Information (FTI)

Federal tax information (FTI) refers to tax return information (TRI) filed by individual taxpayers with the Internal Revenue Service (IRS) and is protected under the IRC. Tax return information held by RRB is that information received directly from the IRS and is subject to stringent safeguarding under the IRC.

Authorities
IRC §. 6103

Guidelines
IRS Publication 1075

First party request

A request made by the subject individual. That is, a request made by an individual for one or more of the records relating to him or her that are maintained in a Privacy Act system of records. It includes requests made by the subject individual regardless of whether the subject individual cited the Privacy Act, the Freedom of Information Act, both Acts or neither Act.

Furnish

A broad, generic term used to mean an agency providing records, whether or not in a Privacy Act system of records and to any party.

Government-wide System of Records Notice

Government-wide systems of records are published by "oversight" federal agencies and

should be consulted when determining correct descriptions for our current or new systems of records, or when determining if records containing personal information are covered by a routine disclosure. We should use and reference a Government-wide SOR instead of creating one of our own that would be a duplication. We have the same responsibilities for disclosure accounting and recordkeeping for Government-wide SORs that are maintained at RRB as we do for RRB SORs.

Individual

Authorities
The Privacy Act of 1974
20CFR§200.5
OMB Memorandum M-03-22

An individual, for the purposes of the Privacy Act, is "a citizen of the United States or an alien lawfully admitted for permanent residence" and is not a company or corporation. For the purposes of conducting a privacy impact assessment, an "individual" is defined as any natural person regardless of citizenship status.

Information in Identifiable Form

Authorities
The Privacy Act of 1974
20CFR§200.5
OMB Memorandum M-03-22

The Privacy Act of 1974 defines a "record" about an "individual" as: "...any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

Section 208(d) of the E-Government Act of 2002 uses the term "information in identifiable form," which is further described OMB Memorandum M-03-22: "Information in identifiable form" is "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Information 'permitting the physical or online contacting of a specific individual' is the same as 'information in identifiable form.'" (See *Personal Information.*)

Need to Know

An instance under the Privacy Act in which disclosure of a record about an individual may be made to an unauthorized third party, and is restricted "..to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." (See *Disclosures Permitted by the Privacy Act.*)

New System Report

A report required by OMB Circular A-130 to be prepared by Federal agencies whenever they intend to establish a new Privacy Act system of records. The report is sent to OMB and the Congress.

SUBJECT: MANAGEMENT OF INFORMATION PRIVACY FOR INDIVIDUALS

Personal Information

Personally Identifiable Information and Federally-owned Personally Identifiable Information (PII) may or may not also be Information in Identifiable Form, but all are contained within the meaning of the much broader concept of "personal information."

Personally Identifiable Information (PII)

Authorities
OMB Memorandum M 06-19;
OMB Memorandum M-07-16;
OMB Memorandum 9-20-2006;
The 1998 Identity Theft Assumption and Deterrence Act (18 U.S.C. 1028);
Fair and Accurate Credit Transactions Act (15 U.S.C. 1681 et seq.)

The term Personally Identifiable Information emerged after the Privacy Act, has had several descriptions, the most recent of which emphasizes the difference between single elements that can lead to identity theft and other elements taken alone or together with other information that can lead to identity theft. PII may or may not be part of a Privacy Act system of records (see *Individual, System of Records*).

"Personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

A social security number alone is considered to be PII and could be used to commit identity theft. USC 18 § 1028(d) which defines "identification" as any name or number that may be used alone or in conjunction with any other information.

Privacy Impact Assessment

Authorities
H.R. 2458/S. 803 ;
OMB Memorandum M-03-22

Guidelines
Privacy Impact Assessment,
Privacy Impact Assessment Official Guidance

Required by the E-Government Act of 2002, a privacy impact assessment, or PIA, is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed in an IT system or online collection. It is done to ensure the information is handled according to all legal, regulatory, and policy requirements concerning privacy; determine the risks and effects of collecting, maintaining, and disseminating the information; and to examine and evaluate protections and alternative processes for handling the information to mitigate potential privacy risks. (See Privacy Threshold Analysis)

Privacy Threshold Analysis

A tool used to determine if a privacy impact assessment is required, or if privacy conditions have changed and a revised privacy impact assessment is required. (See Privacy Impact Assessment)

Record

This term has different meanings for the purposes of the Privacy Act and the Freedom of Information Act, which are distinct from the terms of "record" and "non-record" as defined in 44 U.S.C. 3301 for the purposes of record disposition activities under the Federal Records Act.

Under the Privacy Act, it means "any item, collection or grouping of information about an individual that is maintained by an agency... that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph."

Under the Freedom of Information Act, the term has a much broader meaning: It includes documents, letters, microfilmed data, minutes of meetings, and any other physical or tangible material which are not already matters of public information. They may, but they need not, contain personal information. The term "record" does not include any matter of information which, although compiled from records, requires the Board to manipulate those records to provide an answer.

An example of a request for a record as opposed to a request for information would be a request for an individual's total compensation and years of service as opposed to a request for an annuity estimate. Once the estimate is compiled and kept, it is a record, but it was not a record until that time.

Routine Use

The disclosure under the Privacy Act of a record in a system of records for a use that is compatible with the purpose for which it was collected.

Federal agencies may disclose records in a system of records, without the consent of the subject individual, if they do so pursuant to a routine use that is published in the Federal Register. (See also "Standard Disclosure.")

Safeguard

Physical, administrative and/or technical protections that prevent harm or injury, ensure security and confidentiality, or provide safe transit.

Standard Disclosure

Standard disclosures are "general" or "blanket" routine uses. Beside those disclosures provided under 5 U.S.C. 552a(b) of The Privacy Act which pertain generally to all of the RRB systems of records (see Twelve Disclosures Under The Privacy Act), the RRB has adopted certain standard disclosures which also pertain generally to these systems of records, unless specifically excluded in a system notice, which are in addition to the particular routine uses listed under each system of records.

Subject Individual

The individual about whom records are maintained in a Privacy Act system of records. (See *Individual.*)

System of Records

A discreet group of records about living individuals collected for a specific purpose under the Privacy Act, which is under the control of a federal agency, and from which information is retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual. (See *Individual.*)

System Manager, also Privacy Act System of Records Manager

The federal official responsible for the system of records under the Privacy Act and to whom the subject individual should address his or her request for access to the records in a given system of records. The name and business address of the system manager is part of the system notice required to be published in the Federal Register.

System Notice, also System of Record Notice (SOR, SORN)

The Privacy Act requires each agency to publish its systems of records (SOR) in the Federal Register in a notice. The notice may pertain to an individual agency's system of records, or in certain cases, may pertain to all federal agencies and is referred to as a Government-wide system of records. This notice describes the SOR using specific information called data elements and is referred to as a "system of records notice (SORN)". All information required in a SORN is included under these elements which are recorded on RRB Form IRM-2 certification by the Privacy Act system of records manager or the CPO.

Unauthorized third party request

A request made by a party (person, organization, or agency) other than the subject individual or a party which is authorized by the subject individual to be furnished one or more records of the subject individual maintained in a Privacy Act system of records. The request may or may not cite the FOIA.

IV. Background: The Laws Covering Information Privacy and Disclosure in the Federal Sector

A. Privacy

The Federal government's information privacy program relies primarily on five statutes which assign to OMB policy and oversight responsibilities.

1. The **Privacy Act** of 1974, as amended, (5 U.S.C. § 552a) sets collection, maintenance, and disclosure conditions; access and amendment rights and

notice and record-keeping requirements with respect to information about certain living individuals retrieved by name or identifier. The Act focuses on four basic policy objectives:

To grant individuals increased rights of access to agency records maintained on them.

To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

To restrict disclosure of personally identifiable records maintained by agencies. (See *Disclosures*)

2. The **Computer Matching and Privacy Protection Act** of 1988 (5 U.S.C. § 552a note) amended the Privacy Act to additionally provide a framework for the electronic comparison of personnel and benefits-related information systems. These provisions:

   - add procedural requirements for agencies to follow when engaging in computer-matching activities;
   - provide matching subjects with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated; and
   - require that agencies engaged in matching activities establish Data Protection Boards to oversee those activities.

   Subsequently, the Computer Matching and Privacy Protection Amendments of 1990 (Pub. L. No. 101-508), further clarified the due process provisions.

3. The **Paperwork Reduction Act** of 1995 (44 U.S.C. § 101 note) and the **Information Technology Management Reform Act** of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. §251 note) linked agency privacy activities to information technology and information resources management. Both assign to agency Chief Information Officers (CIO) the responsibility to ensure implementation of privacy programs within their respective agencies.

4. Section 208 of the **E-Government Act** of 2002 included provisions requiring agencies to conduct privacy impact assessments on new or substantially altered information technology systems and electronic information collections, and post web privacy policies at major entry points to their Internet sites.

B. Freedom of Information Act (FOIA)

The primary law behind information disclosure in the federal sector, promoting open government, is the Freedom of Information Act. The FOIA applies only to records held by federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies.

Generally, RRB is required under the FOIA to disclose records requested in writing by any person. However, we may withhold information pursuant to nine exemptions and three exclusions contained in the statute.

FOIA requires that all government records must be published or made available to the public unless they fall into one of the nine enumerated exemptions in 5 U.S.C. § 552(b). The exemptions are not mandatory bars to disclosure, and therefore an agency – unless otherwise prohibited by a more specific statute – may exercise its discretion to disclose exempted information.

Exemption 1 covers documents that are "specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order."

Exemption 2 protects from disclosure information "related solely to the internal personnel rules and practices of an agency."

Exemption 3 protects information specifically exempted from disclosure by statute, provided that such statute (a) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue or (b) established particular criteria for withholding or refers to particular types of matters to be withheld. Sections 12(d) and 12(n) of the Railroad Unemployment Insurance Act (45 U.S.C. §§ 362(d) and (n)) are incorporated into the Railroad Retirement Act. These provisions prohibit disclosure of personally identifiable information unless one of the exceptions contained in those sections are met. These statutes are Exemption 3 statutes.

Exemption 4 applies to "trade secrets" and to "commercial or financial information obtained from a person and privileged or confidential."

Exemption 5 shields from mandatory disclosure "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."

Exemption 6 covers "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

Exemption 7 protects records or information complied for law enforcement purposes.

Exemption 8 applies to matters that are "contained in or related to examination,

operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulations or supervision of financial institutions."

Exemption 9 applies to "geological and geophysical information and date, including maps, concerning wells."

C. Section 12(d) of the Railroad Unemployment Insurance Act

In addition to these, the privacy protections of Section 12(d) of the Railroad Unemployment Insurance Act control any disclosure of RRB information otherwise permitted under the Freedom of Information Act (FOIA) or the Privacy Act:

"45 U.S.C. § 362. Duties and powers of Board

"...(d) Information as confidential

"Information obtained by the Board in connection with the administration of this chapter shall not be revealed or open to inspection nor be published in any manner revealing an employee's identity: Provided, however, That (i) the Board may arrange for the exchange of any information with governmental agencies engaged in functions related to the administration of this chapter; (ii) the Board may disclose such information in cases in which the Board finds that such disclosure is clearly in furtherance of the interest of the employee or his estate; (iii) any claimant of benefits under this chapter shall, upon his request, be supplied with information from the Board's records pertaining to his claim; and (iv) the Board shall disclose to any base-year employer of a claimant for benefits any information, including information as to the claimant's identity, that is necessary or appropriate to notify such employer of the claim for benefits or to full and fair participation by such employer in an appeal, hearing, or other proceeding relative to the claim pursuant to section 355 of this title. Subject to the provisions of this section, the Board may furnish such information to any person or organization upon payment by such person or organization to the Board of the cost incurred by the Board by reason thereof; and the amounts so paid to the Board shall be credited to the railroad unemployment insurance administration fund established pursuant to section 361(a) of this title."

D. Section 12 (n) of the Railroad Unemployment Insurance Act

"45 U.S.C. § 362. Duties and powers of Board

"(n) Sickness benefits; examinations; information and reports; contracts and expenses for examinations

"An application for sickness benefits under this chapter shall contain a waiver of any doctor-patient privilege that the employee may have with respect to any sickness period upon which such application is based: Provided, That such information shall not be disclosed by the Board except in a proceeding relating to any claim for benefits by the employee under this chapter."

E. Right to Access: The Freedom of Information Act (FOIA) vs. the Privacy Act of 1974, as amended

Although the Freedom of Information Act and the Privacy Act were enacted for different purposes, there is some similarity in their provisions. Both the FOIA and the Privacy Act give people the right to request access to records held by agencies of the federal government. The Privacy Act also provides the right to amendment. The FOIA's access rights are generally given to "any person," but the Privacy Act's access rights are given only to the individual who is the subject of the records sought (if that individual is a U.S. citizen or a lawfully admitted permanent resident alien).

The FOIA applies to all federal agency records, including records with personally identifiable information (PII) not covered under the Privacy Act. The Privacy Act, applies to only those federal agency records that are in "a system of records" containing information about living U.S. citizens or resident aliens.

F. Section 6103(i) of the Internal Revenue Code

The Internal Revenue Service (IRS) discloses certain tax return information (TRI, see also *Federal Tax Information*) to the Railroad Retirement Board to administer non-taxation laws.

26 U.S.C. § 6103(i) primarily permits disclosure of returns and return information to officers and employees of Federal agencies for the administration of Federal non-tax criminal and terrorist-related laws subject to the restrictions imposed by 26 U.S.C. § 6103(i)(1)-(7).

26 U.S.C. 6103(i) is the only section where it may be necessary to distinguish between taxpayer return information and return information (other than taxpayer return information).

As a recipient of TRI, the Railroad Retirement Board must observe the disclosure provisions of the Internal Revenue Code (IRC).

26 U.S.C. § 7213 prescribes criminal penalties for Federal and State employees and others who make illegal disclosures of Federal tax returns and return information (FTI).

Additionally, 26 U.S.C. § 7213A, makes the unauthorized inspection of FTI a misdemeanor punishable by fines, imprisonment, or both.

26 U.S.C. § 7431 prescribes civil damages for unauthorized inspection (see *Browsing*) or disclosure and upon conviction the notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

Finally, 26 U.S.C. § 6103(p)(4) requires external agencies and other authorized recipients of Federal tax return and return information (FTI) to establish procedures to ensure the adequate protection of the FTI they receive.

V. Responsibilities

Senior Official for Privacy

Authorities
Executive Order 13353; OMB Memorandum M-05-08

The RRB Senior Agency Official for Privacy (SAOP) is the Chief Information Officer. The SAOP has authority to consider information privacy policy issues at a national and agency-wide level.

The SAOP also has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

The SAOP has the overall agency-wide responsibility for information privacy compliance, and the authority to consider information privacy policy issues at a national and agency-wide level.

The SAOP ensures that the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws and policies, to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction.

The SAOP takes a central role in overseeing, coordinating, and facilitating the agency's compliance efforts, including: reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date and, where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such procedures.

The SAOP also ensures that the agency's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information.

The SAOP also has a central policy-making role in the development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information.

Chief Privacy Officer

The RRB Chief Privacy Officer (CPO) is located in the Information and Resources Management Center of the Bureau of Information Services and has the primary responsibility for agency privacy program and implementing the authorities of the SAOP. The CPO:

- Assures that the RRB complies with fair information practices as set out in the Privacy Act of 1974, including maintaining RRB's Privacy Act system of records, and initiating reviews at the organizational level.
- Coordinates and carries out the administrative actions required by the Privacy Act and related Office of Management and Budget directives and guidelines, including data calls, and FISMA-related and Privacy Management Reporting.
- Coordinates the safeguarding of Internal Revenue Service information, and takes necessary action for agency compliance with applicable provisions of the Internal Revenue Code.
- Assures that the technologies used by the RRB sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.
- Provides agency-wide privacy guidance and technical assistance, and serves on inter- and intra-agency privacy panels and committees for privacy policy and practices.
- Formulates new and revised privacy-related policy, regulations, administrative and directive circulars.
- Assures compliance with the privacy protection provisions of the E-Gov Act and OMB requirements that include privacy impact assessments and posting of privacy policies.
- Performs duties related to the Computer Matching and Privacy Protection Acts of 1988 and 1990, and acts as Secretary to the Data Integrity Board.

Chief FOIA Officer (General Counsel)

Authorities
Executive Order 13392, OMB Memorandum M-06-04

The RRB has designated the General Counsel as its Chief FOIA Officer. The Chief FOIA Officer has agency-wide responsibility for efficient and appropriate compliance with the FOIA, and keeps the head of the agency, and the Attorney General, appropriately informed of the agency's performance in implementing the FOIA. The Chief FOIA Officer:

- Provides guidance, technical assistance, and general oversight for compliance with the FOIA;
- Serves as the focal point for RRB FOIA activities and as the primary liaison with the Department of Justice on FOIA matters;

- Responds to requests for records that specifically cite the FOIA (except for requests made by subject individuals), determines whether the requested records should be released or withheld, and if to be withheld, denies such requests.
- Handles requests for records that do not specifically cite the FOIA (except for requests made by subject individuals), determines whether the requested records should be released or withheld, and if to be withheld, denies such requests, unless the records would be routinely released or denied according to an organization's disclosure procedure, in which case the request would be handled by the affected organization.
- Determines whether fees should be charged/waived.
- Issues an annual notice to RRB employees reminding them of disclosure restrictions;
- Oversees compliance with 26 U.S.C. § 6103 (Confidentiality of tax return information); and
- Reviews disclosure procedure for conformity with this administrative Circular and the FOIA, PA, and Sections 12(d) and 12(n) of the RUIA.

FOIA Public Liaison

Authorities
Executive Order 13392

The RRB has designated the Assistant General Counsel as its FOIA Public Liaison. FOIA Public Liaisons serve as supervisory officials to whom a FOIA requester can raise concerns about the service the FOIA requester has received from the FOIA Requester Service Center (Center), following an initial response from the Center staff. FOIA Public Liaisons shall seek to ensure a service-oriented response to FOIA requests and FOIA-related inquiries. For example, FOIA Public Liaisons shall assist, as appropriate, in reducing delays, increasing transparency and understanding of the status of requests, and resolving disputes. FOIA Public Liaisons shall report to the agency Chief FOIA Officer on their activities and shall perform their duties consistent with applicable law.

Requester Service Center

Authorities
Executive Order 13392

The Office of General Counsel has been designated as the RRB's FOIA Requester Service Center (Center). The Center shall serve as the first place that a FOIA requester can contact in seeking information concerning the status of the person's FOIA request and appropriate information about the agency's FOIA response. The Center shall include appropriate staff to receive and respond to inquiries from FOIA requesters.

SUBJECT: MANAGEMENT OF INFORMATION PRIVACY FOR INDIVIDUALS

Office of General Counsel

To serve as the liaison with the Department of Justice with respect to litigation brought against the Board under the Privacy Act or the Freedom of Information Act;

To prepare, for approval by the Board, decisions on appeals brought under the Privacy Act or Freedom of Information Act;

To handle all subpoenas for Board records;

To review proposed new Privacy Act systems of records for legal sufficiency and correctness of legal citations in the authority category of the Privacy Act system notice;

To render legal decisions regarding disclosure questions and interpretations of the Privacy Act and Freedom of Information Act.

Privacy Act System Managers

For records in a the Privacy Act system of records for which the manager is responsible:

To handle requests of subject individuals (or parties the subject individuals have authorized to act on their behalf) for access to and a copy of any record about themselves;

To handle requests of subject individuals (or individuals the subject individuals have authorized to act on their behalf) for amendment or correction of records about themselves according to the provisions of the Privacy Act;

To advise the Chief Privacy Officer of proposed new or amended routine uses or of other changes to be made in published system notices;

To ensure, in conjunction with collection instruments under the Paperwork Reduction Act, that proper privacy notice is provided to the individual at the point of collection of protected information;

To safeguard the records in the system;

To account for required disclosures;

To furnish such information to the Chief Privacy Officer as may be necessary for compilation of the agency's annual Privacy Management Report to OMB;

To determine whether fees should be waived for first party and authorized third party requesters when the cost of furnishing the records is $10.00 or more;

To provide job specific training to employees or contractors who are authorized to access or disclose personal information in the system of records under the control of the system manager.

SUBJECT: MANAGEMENT OF INFORMATION PRIVACY FOR INDIVIDUALS

Secretary to the Board

To sign and transmit for the Board submission to the Office of the Federal Register, new or altered systems reports to OMB and the Congress, the Privacy Act and FOIA annual reports, and decisions rendered on appeal under the Privacy Act or the Freedom of Information Act;

To transmit to the Office of General Counsel appeals filed under the Privacy Act or the Freedom of Information Act for preparation of decisions on these appeals.

Data Integrity Board (DIB)

Authorities

5 U.S.C. 552a(u); Basic Board Order No. 1 Section 5; Circular RET (RRB)-2

The DIB will ensure the RRB's compliance with the privacy requirements of the Computer Matching and Privacy Protection Act of 1988 and 1990. The Inspector General and the Senior Official responsible for the implementation of the Privacy Act, as amended, must be members of the Committee; however, the Inspector General may not be chair.

The Chief Privacy Officer acts as Secretary to the DIB.

The Data Integrity Board:

Reviews, approves, and maintains all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with the applicable provisions of the Act and all relevant statutes, regulations, and guidelines;

Reviews all matching programs in which the agency has participated during the year, determines compliance with applicable laws, regulations, guidelines, and agency agreements, and assesses the costs and benefits of such programs;

Reviews all recurring matching programs in which the agency has participated during the year, for continued justification for such disclosures;

Compiles an annual report describing the matching activities of the agency that shall be made available to the public on request, and biennially submits the report to the Office of Management and Budget;

Serves as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

Provides interpretation and guidance to agency components and personnel on the requirements of the Act for matching programs;

Reviews agency record-keeping and disposal policies and practices for matching programs to assure compliance with the applicable provisions of the Act.

Acquisition Management Contract Specialists

Acquisition Management contract specialists:

Ensure that Privacy and Security Federal Acquisition Regulations (FAR) clauses are

incorporated in contract and statement of work language, when protected information may be exposed during contract work, and specify the RRB or Government-wide Privacy Act System(s) of Records in which the protected information is maintained;

Provide annually Section M contract information to the Chief Privacy Officer for Privacy Management Reporting.

Keep the Chief Privacy Officer informed about new contract employees to obtain Information Privacy Certification (IRM-1) and orientation from the CPO.

Contracting Officer (Contract Owner) and Contracting Officer's Technical Representative (COTR)

These employees:

Ensure that Privacy and Security language specified under Federal Acquisition Regulation (FAR clauses) is incorporated in contracts and statements of work, when protected information may be exposed during contract work, and specify the RRB or Government-wide Privacy Act System(s) of Records in which the protected information is maintained;

Keep Chief Privacy Officer informed about new contract employees to obtain Information Privacy Certification (IRM-1) and orientation from the CPO;

Ensure that all privacy and security requirements under the E-Government Act and the Federal Information Security Management Act (FISMA) are met by the contractor, including privacy impact assessments and auditing of contractor premises and systems;

Ensure that at the conclusion of the contract that all federally owned sensitive information has been properly destroyed, returned or accounted for. (See Directive Circular IRM-5 and National Institute of Standards and Technology (NIST) special publications.)

Bureaus and Offices

Bureaus and Offices will:

Consult with the Chief Privacy Officer on proposed new systems of records or changes to existing ones;

Forward immediately all non-first party requests for records that specifically cite the Freedom of Information Act to the Chief FOIA Officer;

Handle other requests for records in accordance with established procedures that comport with this circular;

Furnish such information to the Chief Privacy Officer as may be required for periodic reports to OMB and Congress, or to administer the agency privacy program.

Furnish such information to the Chief FOIA Officer as may be required for completion of the agency's annual FOIA report to OMB and the Congress.

Request the Chief Privacy Officer for a decision on whether to waive fees when the requester is an authorized third party other than a Member of Congress and the cost of furnishing the records is $10.00 or more.

VI. Maintenance of Information

A. The Privacy Act

1. The RRB will "...maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." *Authorities* *5 U.S.C. § 552a(e)(7)*

2. The RRB will "...maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." *Authorities* *5 U.S.C. § 552a(e)(1)*

3. The RRB will "...collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." *Authorities* *5 U.S.C. § 552a(e)(2)*

4. The RRB will "...maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual." *Authorities* *5 U.S.C. § 552a(e)(5)*

5. The RRB will "...inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual -- (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information." *Authorities* *5 U.S.C. § 552a(e)(3)*

B. Managing Current Holdings of Personally Identifiable Information (PII)

Authorities
OMB Memorandum M-07-16

Bureaus and offices will regularly monitor their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.

This is a specific expansion of the recordkeeping reporting requirement as defined in OMB Circular A-130, Appendix I, and is intended to reduce the volume of retained PII to the minimum necessary so that it is not held beyond its scheduled retention period or normal usefulness.

The longer records are held beyond their scheduled retention period, the greater the risk of improper disclosure. These records are subject to release under the Freedom of Information Act (FOIA) which could lead to litigation costs.

Further, bureaus and offices should examine their processes to foster information reuse and avoid redundancy of collected or retained PII. By collecting only the information necessary and managing it properly, RRB can reduce the volume of information it possesses, the risk to the information, and the burden of safeguarding it.

VII. Disclosure of Information

A. Personally identifiable information test

The first consideration is if the request is for records contained in a Privacy Act system of records, or otherwise involves personally identifiable information about living U.S. citizens or legal resident aliens.

If yes, the second consideration is whether or not the request is a first party request, a third party request that is authorized, or a third party request that is not authorized.

For unauthorized third party requests, the third consideration is whether or not the request cites the FOIA.

For requests for records not in a Privacy Act system of records, the initial consideration is whether or not the request cites the FOIA.

Finally, all requests for tax return information, or any requests for information that would include a disclosure of tax return information, are to be submitted to the Chief FOIA Officer.

B. The Disclosures Permitted by the Privacy Act

The RRB may not disclose any record which is contained in a Privacy Act system of records by any means of communication to any person, or to another agency, unless it possesses a written authorization by the individual to whom the record pertains, or unless disclosure of the record would be:

1. To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their official duties. (*See* definition of "Need To Know")
2. A required Freedom of Information Act disclosure; the Privacy Act never prohibits a disclosure that the FOIA requires, if there is no FOIA exemption or unless prohibited by Section 12(d).
3. For a routine use described in the Privacy Act system of records notice in which the record is maintained (see definition of Routine Use and Standard Disclosure);
4. To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;
5. To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
6. To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
7. To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
8. To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
9. To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
10. To the Comptroller General, or any of his authorized representatives, in the

course of the performance of the duties of the Government Accountability Office;

11. Pursuant to the order of a court of competent jurisdiction; or
12. To a consumer reporting agency in accordance with Section 3711 (e) of Title 31."

C. Section 12(d) Test

The RRB is restricted as a Federal agency with respect to the disclosure of information and records which pertain to an individual and which identify the individual to whom they pertain by section 12(d) of the Railroad Unemployment Insurance Act (45 U.S.C. § 362(d)), which is incorporated into the Railroad Retirement Act by section 7(b)(3) of that Act (45 U.S.C. § 231f(b)(3)). Section 12(d) provides, in pertinent part, as follows:

Information obtained by the Board in connection with the administration of this Act shall not be revealed or open to inspection nor be published in any manner revealing an employee's identity: *Provided, however,* That (i) the Board may arrange for the exchange of any information with governmental agencies engaged in functions related to the administration of this Act; (ii) the Board may disclose such information in cases in which the Board finds that such disclosure is clearly in furtherance of the interest of the employee or his estate; (iii) any claimant of benefits under this Act shall, upon his request, be supplied with information from the Board's records pertaining to his claim and (iv) the Board shall disclose to any base-year employer of a claimant for benefits any information, including information as to the claimant's identity, that is necessary or appropriate to notify such employer of the claim for benefits or to full and fair participation by such employer in an appeal, hearing, or other proceeding relative to the claim pursuant to section 5 of this Act;* * *.

Section 12(d) is a statute that prohibits disclosure, and thus the personally identifiable information gathered by the Board regarding individuals is exempt from disclosure under exemption 3 of the Freedom of Information Act (5 U.S.C. § 552(b)(3)). Section 12(d) precludes disclosure regarding an individual unless in the judgment of the Board disclosure would clearly be in furtherance of the interest of the named individual or his or her estate.

D. Section 12(n) Test

Medical records maintained by the Board are subject to the restrictions on disclosure imposed under section 12(n) of the Railroad Unemployment Insurance Act (45 U.S.C. § 362(n)), which is also incorporated into the Railroad Retirement Act by section 7(b)(3) of the latter Act (45 U.S.C. § 231(f)(b)(3)), and which provides, in pertinent part, as follows:

"Any doctor who renders any attendance, treatment, attention, or care, or

performs any examination with respect to a sickness of an employee, upon which a claim or right to benefits under this Act is based, shall furnish the Board, in such manner and form and at such times as the Board by regulations may prescribe, information and reports relative thereto and to the condition of the employee. * * * Provided, that such information shall not be disclosed by the Board except in a proceeding relating to any claim for benefits by the employee under this Act."

Section 12(n) prohibits disclosure of medical records under any circumstances other than in connection with a proceeding relating to a claim for benefits under the Acts administered by the Board. In accordance with the Privacy Act (5 U.S.C. § 552a), however, the Board has adopted regulations which provide for the disclosure of medical records to the individual to whom they pertain. Under the Board's regulations, such reports can be disclosed only to the subject individual (see 20 CFR 200.5). The subject individual may, of course, release the records in his possession to anyone.

E. First party requests

It is the RRB policy to grant *subject individuals* access to the records which the Board maintains on them, with the exception of medical records where special rules were established. See 20 CFR § 200.5(e).

Therefore, whether a request cites the Privacy Act, the Freedom of Information Act, both Acts or neither Act, is not material for deciding whether to grant access except when the request involves medical evidence, the request is for records contained in investigation files maintained by the Office of Inspector General, or the request is for personnel background/security records maintained by the Bureau of Human Resources or the Director of Administration. Special rules apply for these exceptions—See 20 CFR § 200.5 regarding the "Protection of privacy of records maintained on individuals." Access is granted in all other cases unless precluded by Section 12(d).

System managers will handle all first party requests for records contained in their respective systems, except as described below, but may delegate such authority to facilitate the granting of access, e.g., the Director of Programs has delegated to field offices the authority to handle most first party requests with respect to records of the subject individual in their possession.

Requests for investigative files maintained by the Office of Inspector General shall be referred to that office.

OPM investigation reports maintained by the Bureau of Human Resources or the Director of Administration are covered by an OPM Privacy Act system of records, which has been exempted from full access by the subject individual. First party requests are forwarded to OPM for reply.

F. Third party requests (authorized)

Authorized third party requests may be of two types. Both types must meet the consent-of-the-subject-individual requirement of the Privacy Act.

1. Request by a third party for records of the subject individual whereby the third party furnishes a document in which the subject individual authorizes, in writing, the Board (and possibly other organizations as well) to furnish the third party with certain of the subject individual's records. Most authorized third party requests are of this type.
2. Request by the subject individual authorizing and directing that the Board furnish a third party with certain records of the subject individual.

System managers should handle such requests as they do first party requests, except that different rules apply with respect to medical records.

G. Third party requests (unauthorized)

1. *Request cites the FOIA*

   a. Receiving organization (if other than the Chief FOIA Officer)

      1). Refer request to Chief FOIA Officer.

      2). Furnish information to requester upon notification from Chief FOIA Officer and send a copy of transmittal letter to Chief FOIA Officer.

   b. Chief FOIA Officer

      1). Review request to determine whether it can be granted in full, denied in part, or denied in full.

      2). If request must be denied in full, notify requester of decision.

      3). If request must be denied in part and granted in part:

         a). Notify requester of decision, request affected bureau(s) or office(s) to furnish records to the requester, and track for notification that records were furnished; OR

         b). Obtain the records to be disclosed, notify requester of decision, and furnish records that must be disclosed along with a notification of the decision.

      4). If request must be granted in full (all the requested records must be disclosed):

         a). Advise the requester that request has been granted and that all the requested records will be furnished under separate cover, request the affected bureau(s) and office(s) to furnish the

information to the requester, track for notification that information has been furnished; OR

b). Obtain the records to be disclosed and furnish them to the requester.

2. *Request does not cite the FOIA*

a. Receiving organization (if other than the Chief FOIA Officer)

1). Determine whether the records requested are under the jurisdiction of the receiving organization; if not, refer request to organization having jurisdiction.

b. Organization having jurisdiction of records

1). The records requested contain personal information about individuals.

a). If the records are maintained in an RRB or Government-wide Privacy Act system of records, release the information to the requester upon receipt of sufficient identity proof only if the applicable system of records notice permits routine disclosure for that type of request. Redact information about individuals not requested or not covered by the routine use that may also be present in the records released. When in doubt, refer the request to the Chief Privacy Officer.

b). If there is no routine disclosure under the Privacy Act permitted above, or if the records are not part of a Privacy Act system of records, refer the request to the Chief FOIA Officer.

2). The records requested do not contain personal information about individuals.

a). Determine whether records would be routinely disclosed or withheld according to the organization's disclosure procedure.

b). If the records would be routinely disclosed, disclose the information.

c). If the records would be routinely withheld under the FOIA, deny the request, cite the section of the FOIA that permits withholding, and advise requester of his or her appeal rights.

d). If it is not clear whether the records should be disclosed or withheld, refer request to the Chief FOIA Officer.

3). Request is for any of the following categories of records:

a). Copies of the Railroad Retirement Act, the RUIA or any other public law affecting operations of the Board, regulations, the Board's annual report, or any other document which is available for sale through the U.S. Government Printing Office or appears on a federal website.

Advise the requester that documents are available for inspection at the Board's headquarters or on the Internet, or may be purchased from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C.

b). Records prepared by the Board for public distribution such as press releases, fact sheets, pamphlets, booklets, brochures, and forms.

Furnish such records as part of the Board's general effort to be responsive to the public.

c). Administrative staff manuals and instructions to staff that affect any member of the public, final opinions and orders, and statements and interpretations of policy not published in the Federal Register, and the index to such items.

Advise requester that such records (with personal identifying information deleted where disclosure would represent a clearly unwarranted invasion of personal privacy) are available for inspection and copying at the offices of the Board, 844 N. Rush Street, Chicago, IL 60611-2092. If the request is received in a district office that possess the requested records, advise requester that such records are available for inspection and copying at the district office.

d). Board promotion panel records maintained in the Bureau of Human Resources:

Refer to the Chief FOIA Officer.

H. Federal Tax Information Received under 26 U.S.C. 6103(i)

If a request is received concerning federal tax information or tax return information received by the RRB under 26 U.S.C. 6103(i), do not disclose any information, and forward the request to the Chief Privacy Officer.

VIII. Privacy Act Systems of Records

A. Notice Requirements at the Time of Collection

The RRB will "...inform each individual whom it asks to *Authorities*

supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual -- (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information." *5 U.S.C. § 552a(e)(3)*

B. System Notice Requirement

The RRB will "...[subject to notice and comment], publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include -- (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its contents; and (I) the categories of sources of records in the system." ***Authorities*** *5 U.S.C. § 552a(e)(4)*

C. Elements Required by the Federal Register

System managers and the CPO will record the system of record notice information on RRB Form IRM-2 for each new system, revisions to existing systems, or when requested by the CPO for biennial or other special reviews. Form IRM-2 contains all of the elements required by the Federal Register, and may be emailed to the CPO as an attachment, or filed in an intranet location designated by the CPO.

D. Accuracy and Relevancy of Records

The RRB will "...maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." ***Authorities*** *5 U.S.C. § 552a(e)(5)*

E. Individuals' Right to Review and Amend Records About Themselves

Individuals as defined under the Privacy Act (e.g., U.S. ***Authorities***

citizens or legal resident aliens) have the right to review and amend federal records about themselves that are in a Privacy Act system of records. *5 U.S.C. § 552a(d); 20 CFR 200.5(h)*

1. *Right to Access Records Under the Privacy Act*

   The RRB will permit individuals to review and obtain copies of records about themselves which are contained in a system of records maintained by the RRB. If the records are viewed in person at a location of the RRB, the individual may choose to bring along another person to review the records, in which case the individual who is the subject of the records must authorize in writing any discussion of their records in the other's presence.

2. *Right to Amend Records Under the Privacy Act*

   a. The RRB will permit the individual to request amendment of a record pertaining to him and--

      1). acknowledge the request in writing within 10 business days; and

      2) promptly, either--

         a). make any correction of any portion of the record which the individual believes is not accurate, relevant, timely, or complete; or

         b). inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

   b. The RRB will permit an individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

   c. In connection with any disclosure containing information about which the individual has filed a statement of disagreement, occurring after the filing

of the statement under paragraph (3) of this subsection, the RRB will clearly note any portion of the record which is disputed and provide copies of the statement and, if the RRB deems it appropriate, copies of a concise statement of the reasons for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

d. Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

F. Updating an Existing Privacy Act Systems of Records

1. *Altered system report required*

a. The following changes require the submission of an altered system report:

1). An increase in the number or a change in the types of individuals on whom records are maintained. Increase in the number of individuals about whom records are maintained need only be reported when the change significantly alters the character and purpose of the system of records; e.g., normal increases in historical files or other increases in the number of records in a file which can be attributed to normal growth patterns need not be reported. An increase in the number resulting from a change in the scope of the population should be reported.

2). An expansion of the type or categories of information maintained; e.g., a system of records which previously contained only an individual's name, SSN, and benefit is being expanded to include his or her address and telephone number.

3). An alteration of the purpose for which the information is used; e.g., a file currently used to determine eligibility for retirement annuities will be used to determine eligibility for rent and energy subsidies.

4). A change to the equipment configuration (i.e., hardware and/or software) on which the system operates that creates substantially greater access to the records in the system; e.g., the addition to a telecommunications capability which could increase the risk of unauthorized access.

5). The addition of an exemption pursuant to Section (j) or (k) of the Privacy Act. (For practical purposes, such an exemption can be claimed only for investigation files.)

b. Notify the CPO

1). A system manager anticipating any of the above type of changes should notify the Chief Privacy Officer as soon as possible but at least 120 days prior to the date the manager desires or needs to have the changes take effect.

2). OMB instructions require a waiting period of at least 60 days from the date of the notice to OMB and the Congress before the changes can be put in effect.

Giving at least 120 days notice will afford the Chief Privacy Officer 60 days in which to prepare the necessary altered system report and Federal Register submission package, as well as allow sufficient time for review by the Director of Administration's office and the Board Members' offices and will provide for the necessary lead time for the Office of the Federal Register.

3). System managers uncertain as to whether a planned change in a system of records would require the submission of an altered system report should consult the Chief Privacy Officer.

c. *Requesting a Waiver*

OMB procedures allow for an agency to request a waiver of the 60 day advance notice requirement in compelling circumstances--when a delay of 60 days would not be in the public interest. The agency must furnish an explanation of the probable effects of OMB not granting the waiver as well as why earlier notice to OMB and the Congress was not provided.

Examples of compelling circumstances which may form the basis for requesting a waiver include the following: the health or safety of individuals is affected, certain statutory requirements must be met, unfair harm may befall a class of individuals.

d. *Routine uses*

Addition of a new routine use or modification of an existing routine use that would expand the scope of the disclosure routinely permitted.

1). The Privacy Act requires that no disclosure may be made pursuant to a routine use until 40 days have elapsed from the date the notice of the proposed routine use is published in the Federal Register.

The purpose of this requirement is to make the public aware of the intended disclosure and allow them 30 days to comment on the proposal before it becomes effective.

Also, 10 additional days are allowed for comment or approval by OMB. Once published, routine uses become effective, as proposed, 40 days after publication unless the agency receives comments that

would result in a contrary determination.

2). System managers intending to establish a new routine use or modify an existing one that would expand the scope of the routinely permitted disclosure should advise the Chief Privacy Officer at least 90 days prior to the intended effective date.

This 90 day notice will allow the Chief Privacy Officer sufficient time to prepare the Federal Register submission, as well as allow sufficient time for review by the Executive Committee and The Board as well as lead time for the office of the Federal Register.

3). There is no waiver of the 40 day waiting period for routine uses.

4). Upon receipt of a notice of a proposed routine use, the Chief Privacy Officer will review the routine use for (a) compatibility with the purposes for which the information to be routinely disclosed was collected; (b) non-contradiction with sections 12(d) and 12(n) of the RUIA; and (c) correctness of format.

5). Should the Chief Privacy Officer have a problem with the routine use as proposed, the Chief Privacy Officer will discuss the problem with the staff person designated by the system manager.

Usually, such discussion will be sufficient to resolve the problem. If not, the Chief Privacy Officer will communicate to the system manager outlining the Officer's reasons why the routine use cannot be added or revised as submitted. The system manager may appeal the CPO's decision to the General Counsel who will issue a final decision.

e. *All other changes*

1). Changes in the following categories which are made to reduce ambiguity, better express what is being done, or reduce the scope of the category (e.g., to delete an item of information maintained on an individual) become effective immediately upon publication in the Federal Register (there is no waiting period for public comment before the change is effective):

"Individuals covered by the system";

"Categories of records";

"Routine uses of records maintained in the system";

"Retrievability."

2). Changes in other categories in the system of records notice such as "name of system," or system manager(s) and address" become effective immediately upon publication in the Federal Register.

3). A memorandum to the Chief Privacy Officer advising of such changes may be made at any time.

G. Adding a Privacy Act Systems of Records

A new system of records requires the submission of a new system report to OMB and the Congress as well as a publication of a new system notice in the Federal Register. The Chief Privacy Officer will prepare the required report and notice with the assistance of the staff of the affected organization.

Bureaus and offices anticipating the need to establish a new system of records should consult with the Chief Privacy Officer at least 120 days prior to the intended effective date.

The waiting period is the same as for the altered report; namely 60 days from the date of the notice to OMB and the Congress.

An agency may request that the 60 day notice period be waived; the requirements are the same as for an altered system report.

Although the 60 day notice may be waived by OMB, such a waiver does not eliminate the requirement that the system be published in the Federal Register and that a new system report be sent to OMB and the Congress.

Also, if the new system contains any routine uses, no disclosures may be made pursuant to such routine uses until 30 days have elapsed from the date the notice of the proposed use is published in the Federal Register. This applies even if OMB waives the 60 day advance notice.

IX. Computer Matching Activities

A. Guidance

The complex and specialized provisions of the Computer Matching and Privacy Protection Act of 1988 and the Computer Matching and Privacy Protection Amendments of 1990, which modified the Privacy Act, are addressed in OMB guidance.

Authorities

OMB Memorandum June 21, 2000;
OMB Federal Register Notice April 23, 1991;
OMB Federal Register Notice June 19, 1989;
OMB Circular A-130, Appendix I

B. Responsibilities

The RRB engages in computer match activities with Federal and State agencies. If RRB is the recipient or benefiting party, it is responsible for developing agreements, renewals, publishing notices in the Federal Register and reporting to Congress and OMB. If the other agency is the benefiting party, it assumes these roles and RRB

provides coordination and support.

Bureaus and offices initiate, coordinate, develop and engage in new or altered, or maintain existing computer matching agreements and data exchange activities with other agencies, perform necessary cost-benefit analyses, and, except for State agreements, establish if conditions are met to renew agreements after the current term expires.

Bureaus and offices will consult with the Chief Privacy Officer and the Chief Security Officer to ensure privacy and security issues are properly addressed in the agreements and in data exchange activities.

The Office of General Counsel reviews new and altered agreements from bureaus and offices for conformance with the Privacy Act, as amended, and other law and guidance.

The RRB Data Integrity Board reviews and approves all computer matching agreements and any continuation of agreements. The Secretary to the RRB Data Integrity Board coordinates all DIB activities, prepares submissions to Congress, OMB and the Federal Register, and also establishes if conditions are met to renew State agreements after the current term expires.

C. Terms of Agreement

In general, the term of the agreement is for 18 months, with a 12-month one-time renewal upon receipt of certification that the agreement will continue unchanged during the renewal period. Continuation of agreements after this term require a new agreement and cost-benefit analysis. Terms of agreements with State agencies may vary from this model.

The effective date of new or altered agreements is 30 days following the date on which notice is given to OMB and the Congress.

For the purposes of filing a notice in the Federal Register, or performing a cost-benefit analysis, State matches are considered to be a single computer matching program.

X. Reporting

A. FISMA and Privacy Management Reporting (Annual)

Beginning fiscal year 2006, the Privacy Management Report (PMR) to the Office of Management and Budget (OMB) is submitted at the end of the fiscal year with the Federal Information Security Management Act (FISMA) report using the guidelines and templates provided by OMB. The RRB is not currently required to submit quarterly FISMA or PMR reports.

For the purpose of reporting and periodic reviews, the Fiscal Year will include

information gathered from September 1 through August 31. For example, Fiscal Year 2008 reporting would include information from September 1, 2007 through August 31, 2008.

B. Privacy Awareness Program

Each year, the CPO releases an email safeguarding awareness request to all employees requiring a certification by email response that they understand the contents of the email and agree to safeguard federally-owned, personally identifiable information, as well as sensitive business information.

Failure to respond or agree may result in the suspension of RRB information system privileges.

C. Privacy Certification by Contractors

Contractors of the RRB who may be exposed to personal or sensitive business information receive privacy orientation by the CPO and provide an information privacy certification on Form IRM-1. Failure to provide this certification may result in suspension of contract activities or access to RRB information systems or services.

D. Periodic Privacy-related Reviews

The Privacy Act requires periodic reviews of privacy-related activities, which have been further described for agencies in OMB Circular A-130 and other guidance.

1. System managers will review the notice language for each system of records for accuracy and completeness every two years (beginning Fiscal Year 2006 on even years) or as requested by the CPO, and document their review on Form IRM-2 submitted to the CPO for acceptance and publishing in the Federal Register. Also, review every four years any system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.
2. At least annually, system managers will also review disclosures of information to ensure that they are proper and sufficiently documented. If any improper disclosure has occurred, the CPO will be notified immediately and the system manager will initiate remedial action for any insufficiencies.
3. Annually, system managers will review the job-specific training required for persons who are authorized to access, use, or modify the Privacy Act systems of records for which they are responsible, as well as the accuracy of the job classes that are authorized to use the system(s).
4. Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.

6. Annually, as part of the Privacy Management Report, and periodically when systems or information collections change, system owners review privacy impact assessments (PIAs) for Major Applications.
7. Biennially, or upon initiation or revision of contract in which a Privacy Act system of records will be used, accessed, or maintained, system managers will ensure that Section M (e.g., 5 U.S.C. 552a(m)(1))contracts conform to FISMA and E-Government Act requirements, that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees, and keeping privacy impact assessments current.
8. Annually, as part of the Privacy Management Report, review agency progress concerning reduction of the unnecessary use of social security numbers (SSN).
9. Biennially, review agency recordkeeping and disposal policies and practices in order to assure compliance with the Privacy Act, paying particular attention to the maintenance of automated records. Annually, ensure that records or important non-records containing personally identifiable information are not retained beyond their stated normal usefulness, and disposed of properly when no longer useful.

E. FOIA (Annual)

Pursuant to 5 U.S.C. § 552(e) of the Freedom of Information Act, the RRB submits an annual report to the Office of Information and Privacy within the Department of Justice. Additionally, the OGC issues annually a Freedom of Information Act Awareness Notice to all employees.

F. Computer Matching

1. *Annually*

   Bureaus and offices will maintain information about computer matching related activities, including reviews, and provide them to the CPO for the Privacy Management Report data call.

   The CPO, on behalf of the DIB, will compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including:

   a. matching programs in which the agency has participated as a source agency or recipient (requesting) agency;

   b. matching agreements proposed under subsection (o) that were disapproved by the Board;

   c. any changes in membership or structure of the Board in the preceding

year;

d. the reasons for any waiver of the requirement for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

e. any violations of matching agreements that have been alleged or identified and any corrective action taken; and

f. any other information required by the Director of the Office of Management and Budget to be included in such report.

2. *Biennially*

As required by The Computer Matching and Privacy Protection Acts of 1988 and 1990, OMB Circular A-130, and OMB memorandum of June 21, 2000, in even years, the RRB Data Integrity Board submits to the Office of Information and Regulatory Affairs, OMB, a report of computer matching activities compiled above for the preceding two calendar years.

G. Accounting of Disclosures

1. *Requirements*

Bureaus and offices are required to:

a. Keep an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person or agency and of the name and address of the person or agency to whom the disclosure is made, with the exception of disclosures:

1). made internally to employees on a "need to know" basis;

2). required under the FOIA pursuant to an actual request.

b. Retain the accounting for at least 5 years after the disclosure to which the accounting is made or the life of the record, whichever is longer.

c. Except for the following disclosures, make the accounting available to the subject individual on his or her request:

1). disclosures to another agency for civil or criminal law enforcement;

2). disclosures made from a system of records exempted from this accounting requirement. (Currently the only RRB system of records so exempted is RRB-43, Investigation Files, maintained by the Office of the Inspector General).

d. Inform the prior recipients of records in a Privacy Act system of records about any correction or notation of dispute when, in response to a request by the subject individual to amend his or her record, the agency

corrects the record or allows the filing of a statement of dispute.

2. *Accounting for Third Party Disclosures and Denials*

   a. Privacy Act system of records managers must ensure that they are accounting for disclosures of information from their systems, to establish whether or not the disclosures were proper:

      1). the language of the original inquiry,

      2). the identity and relationship of the requester (and how that was proved),

      3). the purpose to which the requested information will be put,

      4). whether or not a reference to the Privacy Act was made,

      5). whether the information is required to be released under FOIA,

      6). whether the information is precluded from release under the Internal Revenue Code or Section 12(d) of the RUIA,

      7). the Privacy Act system of records in which the protected information is maintained,

      8). the routine use provided by the Privacy Act, RRB standard disclosure, or the applicable system of records notice that was applied to release the information in lieu of a signed release statement by the individual who is the subject of the information.

   b. Third party disclosures may be made individually or in bulk, as in computer matching programs.

   c. For administrative convenience, disclosures that would be required under the FOIA will be accounted for, even though the Privacy Act does not require such accounting. Therefore, for the purposes of FOIA reporting, all first party requests are both Privacy Act requests and FOIA requests. All requests for access to records, regardless of which law is cited by the requestor, will be accounted for.

   d. Manual disclosures occur when the request is made for one or more records for a given individual and the disclosure is made manually, by completion of a form or a letter.

   e. Mass disclosures occur when records are disclosed in an IT environment, such as email, file transfer or electronic media. Disclosure accounting is required, and includes:

      1). Recurring approved disclosures as part of a computer match agreement between the RRB and another government entity.

      2). One-time mass disclosures, such as requests for lists of deceased

beneficiary names, dates of death and social security numbers (these require approval by the Chief FOIA Officer).

g. Improper Disclosure.—Upon discovery of an improper disclosure, immediately notify the CPO.

3. *Procedures*

System managers are responsible for developing and implementing procedures to meet the accounting requirements, so they may provide information annually for Privacy Management Reporting, or for management reviews.

XI. Fees

A. FOIA

The Freedom of Information Act provides that:

1. Federal agencies shall issue regulations specifying a uniform schedule of fees;
2. Fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;
3. Fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media;
4. For any request not described in...2. and 3. above, fees shall be limited to reasonable standard charges for document search and duplication.
5. For any request described in 3. and 4. above, no charge may be made for the first two hours of search time or for the first 100 pages of duplication.
6. Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review.
7. Documents shall be furnished without any charge or at charge reduced below the fees established if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.
   a. Such charges shall be limited to reasonable standard charges for document search and duplication and provide for recovery of only the direct costs of such search and duplication; and

b. Documents shall be furnished without charge or at a reduced charge where the agency determines that waiver or reduction of the fee is in the public interest because furnishing the information can be considered as primarily benefiting the general public.

B. Privacy Act

The Privacy Act provides that Federal agencies issue regulations to establish fees to be charged, if any, to any individual for making copies of their record, excluding the cost of any search for and review of the record.

C. Board regulations

1. *FOIA*

a. The Board's regulations on implementing the FOIA (20 CFR §200.4(g)) provide that to the extent fees are chargeable they are chargeable in accordance with the following schedule:

1). The fee for copies shall be $.15 per page.

2). The charge for making a manual normal search for records shall be the salary rate, including benefits, for a GS-7, step 5 Federal employee.

3). The charge for reviewing documents to determine whether any portion of any located document is permitted to be withheld shall be the salary rate, including benefits, for a GS-13, step 5 Federal employee.

4). Computer charges shall be the actual per hour/per minute cost.

b. For the purpose of assessing fees, requesters shall be grouped into one of the following categories:

1). Commercial use requesters will be charged in full for the cost of searching, reviewing, and copying and shall not consider a request for waiver or reduction based on an assertion that disclosure would be in the public interest.

2). Educational and non-commercial scientific institution requesters will be charged for the cost of reproduction alone, excluding the cost of the first 100 pages, for which no charge will be made.

3). Representatives of the news media will be charged for the cost of reproduction alone, excluding the cost of the first 100 pages, for which no charge will be made.

4). Individuals, who are the subject of records in Privacy Act Systems of Records, will be charged under the fees provisions of the Privacy Act

in 2, below.

5). All other requesters will be charged the full direct cost of searching for and reproducing records that are responsive to the request, except that the first 100 pages of reproduction and the first 2 hours of search time shall be provided without charge.

2. *Privacy Act*

RRB regulations implementing the Privacy Act provide that we may assess a fee for copies of any records furnished the subject individual or an authorized third party. The fee shall be the actual cost per page. Any fees of less than $10.00 may be waived by the Privacy Act system manager if it is determined by the system manager that it is in the public interest to do so.

3. *Charging Fees*

Authorities
20 C.F.R. § 200.3(g)

Regardless of whether the requester is a 1st party or 3rd party requester, if the total cost of allowable search, review, and duplication photocopying, computer time
and search time (where applicable) is less than $10.00 per request, no fees will be charged.

If the requester is a Member of Congress, no fees will be charged.

If the requester is the subject individual or an authorized third party and the cost is $10.00 or more, the system manager will determine whether the fee will be waived.

If the requester is an unauthorized third party or the request is for records not in a Privacy Act system of records and the cost is $10.00 or more, the Chief FOIA Officer will determine whether the fee should be waived or reduced because furnishing the information is "likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester" can be considered as primarily benefiting the general public. To expedite the determination, organizations handling such a request may contact the Chief FOIA Officer. If a fee will be charged, the requester should be furnished with an extra copy of the RRB's response and advised to include that copy with the check.

Payment of fees may only be made by check or money order, made payable to "U.S. Railroad Retirement Board." Deliver the payment, with a description of what it is for, to the Treasury Section of the Bureau of Fiscal Operations.

XII. Privacy Impact Assessments

Authorities
E-Government Act of 2002
OMB Memorandum M-03-22;

Guidelines
Privacy Impact Assessment, Privacy Impact Assessment Official Guidance

Privacy Impact Assessments (PIAs) are required by Section 208 of the E-Government Act of 2002 (E-Gov Act or E-Gov) for all Federal government agencies that develop or procure new technology involving the collection, maintenance or dissemination of information in identifiable form or that make substantial changes to existing technology for managing information in identifiable form.

The Office of Management and Budget (OMB) guidelines to agencies in implementing the privacy portion of the E-Gov Act are contained in OMB Memorandum M-03-22. OMB may require PIAs for major information systems (MIS) necessitated under the E-Government Act when funding is requested. Agencies also must report to OMB about PIAs in their periodic FISMA and Privacy Management Report (OMB Circular A-130, Appendix I) or when submitting information collection clearances required under the Paperwork Reduction Act.

When a system owner or program manager is preparing to embark on internal or contracted information technology projects or information collection activities, a privacy threshold assessment (PTA) will be provided to the Chief Privacy Officer (CPO) to determine if a new privacy impact assessment (PIA) is required or if an amendment to an existing one is required. Additionally, the CPO will be consulted at any time when the climate or conditions, virtual or actual, surrounding the collection or use of PII have changed.

XIII. Safeguarding

Authorities
Directive Circular IRM-15;

The Privacy Act requires Federal agencies to "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained [in a Privacy Act system of records].."

Personally identifiable information is personal information that may not be contained in a system of records if a unique identifier is not used to retrieve the individual records. However, whether personally identifiable information maintained by the RRB is contained in a system of records or not, it must be safeguarded from improper disclosure or misuse during the entire life cycle of the information, from collection through to final disposition.

SUBJECT: MANAGEMENT OF INFORMATION PRIVACY FOR INDIVIDUALS

A. Tax Return Information

The RRB is required under the Internal Revenue Code to safeguard federal tax return information received from the Internal Revenue Service. This requirement is described in Directive Circular IRM-3, *Safeguarding of Tax Returns and Tax Return Information.*

B. Data Exchange

The preferred method for exchanging personal information in digital form, such as computer match exchanges, is secure FTP or a similar controlled, encrypted process, or secure email (using digital certificates). When using secure FTP, RRB will place request files in the other party's secure FTP area, and retrieve updated response files from there. Web-based encrypted file upload and download may also be considered. When these methods are not possible, media containing exchange data should be encrypted, and delivery should be tracked using a courier service.

C. Remote Use

Remote use involves accessing, or downloading federally-owned information residing in IT systems and accessed via an internet, network, or telecommunication connection, or physically removing federally-owned information stored on paper or digital media from the federally controlled space where it is safeguarded. This includes information that is transmitted from within federally controlled space or email systems to non-federal destinations. Remote use exposes personally identifiable, federally-owned information and places information systems at significant risk of being exploited. Employees or contractors authorized to access or transmit federally-owned information remotely are required to use supplied or approved encryption-protected equipment and connections, and to protect paper and media removed from federally controlled space by encrypting the media and keeping the media or paper that has been removed or produced off-site in locked storage during transfer or when not in use. Materials must be returned to the originating federally controlled space, or disposed of according to Directive Circular IRM-5 if no longer needed.

D. FISMA Compliant IT Systems

To help safeguard personally identifiable information, RRB must meet the requirements of the Federal Information Security Management Act (FISMA) and associated policies and guidance from OMB and the National Institute of Standards and Technology (NIST), including certifying and accrediting agency and contract information systems.

XIV. Penalties

A. Under the Privacy Act

1. *Criminal Penalties*

   a. Any officer or employee of an agency, who knowingly and willfully discloses—in any manner to any person or agency not entitled—agency records containing individually identifiable information the disclosure of which is prohibited, shall be guilty of a misdemeanor and may be fined not more than $5,000.

   b. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements shall be guilty of a misdemeanor and may be fined not more than $5,000.

   c. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and may be fined not more than $5,000.

B. Under the Internal Revenue Code

1. *Criminal Penalties*

   a. For willful, unauthorized disclosure: upon conviction, a fine not exceeding $5,000, or imprisonment not exceeding 5 years, or both, plus costs of prosecution. In addition, upon conviction, the employee shall be dismissed from Federal employment.

   b. For willful, unauthorized inspection: upon conviction, a fine not exceeding $1,000, or imprisonment of not more than 1 year, or both, plus the costs of prosecution. In addition, upon conviction, the employee shall be dismissed from Federal employment.

2. *Civil Penalties*

   Upon conviction, an amount payable to the plaintiff equal to the sum of

   a. the cost of the court action, plus

   b. the greater of—

      1). $1,000 for each act of unauthorized inspection or disclosure, or

      2). the sum of --

         a). the actual damages sustained by the plaintiff, plus

         b). "in the case of willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive

damages."

C. Administrative Actions

In addition to any civil or criminal penalties cited above, an employee who improperly maintains, accesses or discloses protected information may be subject to suspension or removal from their position. (See RRB Employee Handbook, Disclosures of Information; Directive Circular IRM-15).

XV. Effective Date

This circular supersedes Directive Circular IRM-2 (3-86), July 1, 1986, and will remain in effect until rescinded or revised.