(NIST) guidelines, including network monitoring, defenses in-depth, incident response and forensics.

RETENTION AND DISPOSAL:

Retained and disposal in accordance with National Archives and Records Administration (NARA), General Record Schedule, GRS–1, Item #29, Employee Training Records, Destroy when 5 years old or when superseded or obsolete, whichever is sooner.

SYSTEM MANAGER(S) AND ADDRESS:

Director of Human Resources, Office of Administration, U.S. Railroad Retirement Board, 844 North Rush Street, Chicago, Illinois 60611–2092.

NOTIFICATION PROCEDURE:

Requests for information regarding an individual's record should be in writing addressed to the System Manager identified above, including the full name of the individual. Before information about any record will be released, the System Manager may require the individual to provide proof of identity or require the requester to furnish an authorization from the individual to permit release of information.

RECORD ACCESS PROCEDURE:

See Notification section above.

CONTESTING RECORD PROCEDURE:

See Notification section above.

RECORD SOURCE CATEGORIES:

RRB employees.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

* * * * *

RRB–59

SYSTEM NAME:

Electronic Information Systems Activity and Access Records.

SYSTEM LOCATION:

U.S. Railroad Retirement Board, 844 Rush Street, Chicago, Illinois 60611.

SECURITY CLASSIFICATION:

Controlled Unclassified Information (CUI).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals (authorized or unauthorized) who attempt to or access RRB electronic information systems (stand-alone or network based). This includes individuals who send or receive electronic communications, access the internet/intranet, system databases, files or applications or pass electronic traffic through our network infrastructure, to include remote access.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system of records may include:

1. Electronic logs or reports from:
   a. End user information systems,
   b. Network servers or mainframe computer,
   c. Network infrastructure devices,
   d. Network security and management devices, and
   e. Information systems performing contracted services for the agency.
2. Specific data collected may include information about the source, destination or intermediate connections that may contain:
   a. Internet Protocol (IP) address,
   b. Uniform Resource Locator (URL),
   c. Date/Time of attempted or actual log-on,
   d. Date/Time of log-off,
   e. Duration of connection,
   f. Size (amount) and type of data transferred,
   g. Keyword(s) used in internet related searches,
   h. Information system name,
   i. Information system Media Access Control (MAC) address,
   j. Electronic mail addresses and subject,
   k. Files/Applications accessed,
   l. User logon name and passwords, or password hashes, titles, or agency, or
   m. Any other information that is necessary for information systems to connect, authenticate and transfer data.
3. Network security and management devices may capture additional information that is required for them to perform their mission to include complete network monitoring.
4. RRB information system logs generally do not contain personally identifiable information (PII), however incidental collection is possible during system monitoring or other official government purposes.
5. It is possible that during the course of official government business purposes, investigations or monitoring that an individual's name may be associated with an information system or its IP address.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

a. 5 U.S.C. 302, Delegation of Authority to Federal Agencies,
b. 44 U.S.C. 3544, Federal Agency Responsibilities, and
c. 45 U.S.C. 231f(b)(6) and 45 U.S.C. 362(l), Duties and Powers of the Railroad Retirement Board.

PURPOSE(S):

Information in this system of records may be used by any authorized staff member, in the performance of their official duties to assist in the planning, management, troubleshooting, security and investigations of our Federal information systems and supporting network.

Authorized managers or system security staff may use these records to assist them to investigate any potential or actual inappropriate use or any other improper activity by an employee, contractor, or other individual with our information systems. This information may be used to initiate disciplinary, administrative, or civil action. If investigation of the records appears to indicate a violation or potential violation of law, those and any supporting records may be referred to appropriate law enforcement officials for criminal investigation and possible prosecution.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS, AND THE PURPOSES OF SUCH USES:

In addition to the conditions of disclosure listed in 5 U.S.C. 552a(b) of the Privacy Act and the RRB's Standard Disclosures, the RRB may release these records:

a. To provide information to any authorized person(s) to assist in any official investigation involving the unauthorized, or inappropriate use of any RRB information system(s);
b. To an actual or potential party or his or her representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;
c. To any Federal, State, local, or tribal law enforcement agency if information in this system of records may indicate a potential or actual violation of statute, regulation, rule or order issued by their respective governmental agency, and
d. To other government agencies where required by law.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Magnetic disk, magnetic tape, optical or paper media as necessary for official business.

RETRIEVABILITY:

Records can typically be retrieved by any of the data elements below:
a. Internet Protocol (IP) address,
b. Uniform Resource Locator (URL),
c. Date/Time of attempted or actual log-on,
d. Date/Time of log-off,

e. Duration of connection,

f. Size (amount) of data transferred,

g. Keywords used in internet related searches,

h. Information system name,

i. Information system Media Access Control (MAC) address,

j. Electronic mail addresses and subject,

k. Files/Applications accessed,

l. User logon name and passwords, or password hashes, titles, or agency.

We do not typically connect any of the above data with a specific person; however, in some instances conducting official governmental business, a person's name may be connected to any of these data elements.

SAFEGUARDS:

Paper or Optical Media: Maintained in areas not accessible to the public in locking filing cabinets at the RRB. Access is limited to authorized RRB employees. Information that is related to an investigation is secured inside locking safes. Building has 24 hour on-site security officers, closed circuit television monitoring and intrusion detection systems.

Magnetic tape and disks: Computer and computer storage rooms are restricted to authorized personnel and have electronic access controlled doors. On-line query safeguards include a lock/unlock password system, a terminal oriented transaction matrix, role based access controls and audit trail. For electronic records, system securities are established in accordance with National Institute of Standards and Technology (NIST) guidelines, including network monitoring, defenses in-depth, incident response and forensics.

RETENTION AND DISPOSAL:

a. General System/Log Files:

Delete/destroy when one year old or when no longer needed for administrative, legal, audit or other operational purposes.

b. Investigative Files:

(1) Computer Security Incident Handling, Reporting, Follow-up Records, and Investigative Documents. Destroy/delete three years after after all follow up actions are completed.

(2) RRB Criminal Investigations. Maintained by RRB Office of Inspector General (Investigations). RRB Records Disposition Schedule 17, Item # 17–3: Place in inactive files when case is closed. Cutoff inactive files at end of the fiscal year. Destroy 10 years after cutoff.

(3) Other Criminal Investigations. Maintained in accordance with that Law Enforcement Agencies schedule.

SYSTEM MANAGER(S) AND ADDRESS:

Chief of Information Resources Management, Bureau of Information Services, U.S. Railroad Retirement Board, 844 North Rush Street, Chicago, Illinois, 60611–2092.

NOTIFICATION PROCEDURE:

To the extent permitted under the Privacy Act of 1974, (5 U.S.C. 552a) this system of records is exempted from access, notification and correction provisions. The exemption claimed is 5 U.S.C. 552a(k)(2), investigatory material compiled for law enforcement purposes. Additionally, law enforcement investigative material falls under RRB Privacy Act Systems of Records RRB–43 and is generally exempt from release under the reasons stated in that notice. Information in this Privacy Act System of Records is generally not releasable under a Freedom of Information Act (FOIA), 5 U.S.C. 552 exemptions: (b)(2) Risk of Circumvention, (b)(6) Personal Privacy, or (b)(7) Law Enforcement. Individuals (authorized or unauthorized) attempting to access an RRB information system are provided a warning notification that this is an official U.S. Government information system and that they have no expectation of privacy, the system may be monitored and that records of their activity may be used for adverse administrative, civil or criminal action. The individual must acknowledge and accept these conditions via a warning banner when they attempt to log onto the network. Individuals who circumvent or are not provided a log-on banner for whatever reason, are still subject to these provisions.

RECORD ACCESS PROCEDURE:

See Notification section above.

CONTESTING RECORD PROCEDURE:

See Notification section above.

RECORD SOURCE CATEGORIES:

Most records are automatically generated electronically by RRB information systems, or by management officials during the course of official business.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Yes, this is an exempted system. See notification procedures above.

Appendix I

Offices of the U.S. Railroad Retirement Board (refer to *http://www.rrb.gov/field/field.asp* for the most current addresses):

Headquarters: 844 North Rush Street, Chicago, IL 60611–2092.

Office of Legislative Affairs: 1310 G Street Northwest, Suite 500, Washington, DC 20005–3004.

District Offices:

ALABAMA

Medical Forum Bldg., 950 22nd Street North, Room 426, Birmingham, AL 35203–1134.

ARIZONA

Fiesta Square, 1220 South Alma School Road, Mesa, AZ 85210–2098.

ARKANSAS

1200 Cherry Brook Drive, Suite 500, Little Rock, AR 72211–4122.

CALIFORNIA

858 South Oak Park Road, Suite 102, Covina, California 91724–3674.

Oakland Federal Building, 1301 Clay Street, Suite 110S, Oakland, CA 94612–5215.

910 Cirby Way, Suite 100, Roseville, CA 95661–4420.

COLORADO

721 19th Street, Room 177, Post Office Box 8869, Denver, CO 80201–8869.

FLORIDA

550 Water Street, Suite 220, Jacksonville, FL 32202–4411.

Timberlake Federal Building, 500 East Zack Street, Suite 300, Tampa, FL 33602–3918.

GEORGIA

Peachtree Summit Building, 401 West Peachtree Street, Room 1702, Atlanta, GA 30308–3519.

ILLINOIS

844 North Rush Street, Room 901, Chicago, IL 60611–2092.

Millikin Court, 132 South Water Street, Suite 517, Decatur, IL 62523–1077.

63 West Jefferson Street, Suite 102, Joliet, IL 60434–4337.

INDIANA

The Meridian Centre, 50 South Meridian Street, Suite 303, Indianapolis, IN 46204–3538.

IOWA

Federal Building, 210 Walnut Street, Room 921, Des Moines, IA 50309–2116.

KANSAS

Cambridge Plaza Suite, 2020 North Webb Road, Suite 104, Wichita, KS 67206–3408.

KENTUCKY

Theatre Building, 629 South 4th Street, Suite 301, Louisville, KY 40202–2461.