

Prescription Drug, Improvement and Modernization Act of 2003.

We will provide Fiscal Service with a finder file consisting of Social Security Numbers (SSNs) extracted from our Medicare Database (MDB) File System. The MDB File System is a repository of Medicare applicant and beneficiary information related to Medicare Part A, Part B, Medicare Advantage Part C, and Medicare Part D. We may disclose file data from the MDB System pursuant to the "Medicare Part D and Part D Subsidy File" (60-0321), fully published at 71 **Federal Register** 42159 on July 25, 2006 and amended at 72 **Federal Register** 69723 on December 10, 2007.

Fiscal Service will match the SSNs in our finder file with the SSNs in Fiscal Service Savings Securities Registration Systems and return the formatted comparison file. These records reside in the systems of records Treasury/BPD.002, "United States Savings-Type Securities Treasury/BPD" and Treasury/BPD.008, "Retail Treasury Securities Access Application—Treasury/BPD" fully published at 73 **Federal Register** No. 142, pages 42904–2491 on July 23, 2008.

For definitive records (*i.e.*, the actual securities issued in engraved or printed physical form), we will furnish Fiscal Service with the SSN, in a specified format, for each individual for whom we request Savings Securities ownership information. Fiscal Service will disclose the following to us: (a) The denomination of the security; (b) the serial number; (c) the series; (d) the issue date of the security; (e) the current redemption value; and (f) the return date of the finder file.

For book entry records (*i.e.*, securities maintained as computer records on the records of a bank or Fiscal Service), we will furnish Fiscal Service with the SSN, in a specified format, for each individual for whom we request Savings Securities registration information. Fiscal Service bases the query on the SSN associated with the account and reports any subsequent account holdings. When a match occurs on an SSN, Fiscal Service will disclose the following: (a) The purchase amount; (b) the account number and confirmation number; (c) the series; (d) the issue date of the security; (e) the current redemption value; and (f) the return date of the finder file.

E. INCLUSIVE DATES OF THE MATCHING PROGRAM

The effective date of this matching program is April 1, 2016, provided that the following notice periods have lapsed: 30 days after publication of this notice in the **Federal Register** and 40

days after notice of the matching program is sent to Congress and OMB. The matching program will continue for 18 months from the effective date and, if both agencies meet certain conditions, it may extend for an additional 12 months thereafter.

[FR Doc. 2016-04123 Filed 2-25-16; 8:45 am]

BILLING CODE 4191-02-P

DEPARTMENT OF STATE

[Public Notice 9455]

Privacy Act; System of Records: Protocol Records, State-33.

SUMMARY: Notice is hereby given that the Department of State proposes to amend an existing system of records, Protocol Records, State-33, pursuant to the provisions of the Privacy Act of 1974, as amended (5 U.S.C. 552a) and Office of Management and Budget Circular No. A-130, Appendix I.

DATES: This system of records will be effective on April 6, 2016, unless we receive comments that will result in a contrary determination.

ADDRESSES: Any persons interested in commenting on the amended system of records may do so by writing to the Director, Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW., Washington, DC 20522-8100.

FOR FURTHER INFORMATION CONTACT: John Hackett, Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW., Washington, DC 20522-8100, or at Privacy@state.gov.

SUPPLEMENTARY INFORMATION: The Department of State proposes that the current system will retain the name "Protocol Records" (previously published at 78 FR 54945). The information in this system of records is an accounting of those U.S. Government officials receiving gifts and decorations from foreign governments and to record for historical, organizational, and logistical purposes the names of the individuals applying to participate, invited to, supporting, and attending official Department of State functions or other events co-sponsored with the Federal Government or other partners, and to verify individuals nominated as a diplomatic representative on behalf of a foreign government. The proposed system will include modifications to the following sections: System location, Categories of individuals, Categories of records, Purpose, Routine Uses, Safeguards, System managers, and administrative updates.

The Department's report was filed with the Office of Management and Budget. The amended system description, "Protocol Records, State-33," will read as set forth below.

Joyce A. Barr,

Assistant Secretary for Administration, U.S. Department of State.

STATE-33

SYSTEM NAME:

Protocol Records.

SYSTEM CLASSIFICATION:

Unclassified and Classified.

SYSTEM LOCATION:

Department of State, 2201 C Street NW., Washington, DC 20520. Abroad at U.S. embassies, U.S. consulates general, and U.S. consulates; U.S. missions; Department of State annexes; various field and regional offices throughout the United States. Within a government cloud, implemented by the Department of State and provided by a cloud-based software as a service (SaaS) provider.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by this system include those receiving gifts and decorations from foreign governments; individuals invited to and supporting official Department of State functions or other events co-sponsored with the federal government or other partners; applicants for participation and attendees of Department of State conferences or other events co-sponsored with the federal government or other partners; individuals who are part of foreign delegations; individuals working at foreign embassies, missions and organizations; and nominees for foreign ambassadorships to the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system include descriptions of gifts and decorations received from foreign governments; donors; guest lists; type of function; sample invitations; contact information, address and occupation; biographical information (this includes, but is not limited to: Names, nationalities and citizenship, résumés, *curricula vitae*, copies of passports, copies of visas, dates of birth, and photographs), special needs, requests and accommodations, travel arrangements and related information, security information, and application and registration information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

22 U.S.C. 2621, 22 U.S.C. 2625, 22 U.S.C. 4301 *et seq.*

PURPOSE:

The information in this system of records is an accounting of those U.S. Government officials receiving gifts and decorations from foreign governments and to record for historical, organizational, and logistical purposes the names of the individuals applying to participate, invited to, supporting, and attending official Department of State functions or other events co-sponsored with the Federal Government or other partners, and to verify individuals nominated as a diplomatic representative on behalf of a foreign government.

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

The information contained in these records may be shared with:

(a) The Executive Office of the President; Congress; and other government agencies having statutory or other lawful authority to maintain such information.

(b) A contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m);

(c) Nongovernmental organizations, individuals, and panels to review applications and otherwise aid in the selection of participants in Department of State conferences and related functions;

(d) The news media and the public, with the approval of the Chief of Mission or Bureau Assistant Secretary who supervises the office responsible for the outreach effort, provided that the approving official determines that there is legitimate public interest in the information disclosed, except to the extent that release of the information would constitute an unwarranted invasion of personal privacy;

(e) Foreign governments where there is a need to verify the information provided for their delegates;

(f) Other Federal, State, and Local Governments for uses within their statutory missions, which may include law enforcement, transportation and border security, critical infrastructure protection, and fraud prevention; and

(g) Other individuals and organizations applying to, invited to, attending, or supporting a given conference, provided that the subject of the information opts-in to such sharing.

The Department of State publishes periodically in the **Federal Register** its Prefatory Statement of Routine Uses which applies to all of its Privacy Act System of Records. These standard

routine uses apply to Protocol Records, State-33.

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

Electronic and hard copy media.

RETRIEVABILITY:

By an individual name.

SAFEGUARDS:

All users are given cyber security awareness training which covers the procedures for handling Sensitive But Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Foreign Service and Civil Service employees and those Locally Engaged Staff who handle PII are required to take the Foreign Service Institute distance learning course, PA 459, instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly.

Access to the Department of State, its annexes and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All paper records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

Before being granted access to Protocol Records, a user must first be granted access to the Department of State computer system. Remote access to the Department of State network from non-Department owned systems is authorized only to unclassified systems and only through a Department approved access program. Remote access to the network is configured with the Office of Management and Budget Memorandum M-07-16 security requirements which include but are not limited to two-factor authentication and time out function. All Department of State employees and contractors with authorized access have undergone a

thorough background security investigation.

The safeguards in the following paragraphs apply only to records that are maintained in cloud systems. All cloud systems that provide IT services and process Department of State information must be: (1) Provisionally authorized to operate by the Federal Risk and Authorization Management Program (FedRAMP), and (2) specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy. Only information that conforms with Department-specific definitions for Federal Information Security Management Act (FISMA) low or moderate categorization are permissible for cloud usage. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, NIST Federal Information Processing Standards (FIPS) and Special Publication (SP), and Department of State policy and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Authorizing Official.

RETENTION AND DISPOSAL:

Records are retired and destroyed in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA). More specific information may be obtained by writing to the following address: Director, Office of Information Programs and Services, A/GIS/IPS; SA-2, Department of State; 515 22nd Street NW., Washington, DC 20522-8100.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Chief of Protocol for Management and Executive Director, Office of the Chief of Protocol, Department of State, 2201 C Street NW., Washington, DC 20520.

The Director of Major Events and Conferences Staff, Office of Major Events and Conferences, Department of State, 2201 C Street NW., Washington DC, 20520.

NOTIFICATION PROCEDURE:

Individuals who have cause to believe that the Office of the Chief of Protocol or Office of Major Events and Conferences Staff may have records pertaining to him or her should write to the following address: Director; Office of Information Programs and Services, A/ GIS/IPS; SA-2 Department of State; 515 22nd Street NW., Washington, DC 20522-8100.

The individual must specify that he or she requests the records of the Office of the Chief of Protocol or the Office of Major Events and Conferences Staff to be checked. At a minimum, the individual must include the following: Name, date and place of birth, current mailing address and zip code, signature, and any other information helpful in identifying the record.

RECORD ACCESS PROCEDURES:

Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director; Office of Information Programs and Services (address above).

CONTESTING RECORD PROCEDURES:

(See above).

RECORD SOURCE CATEGORIES:

These records contain information collected directly from: The individual who is the subject of these records; employers and public references; other officials in the Department of State; other government agencies; foreign governments; and other public and professional institutions possessing relevant information.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 2016-04192 Filed 2-25-16; 8:45 am]

BILLING CODE 4710-24-P

SURFACE TRANSPORTATION BOARD

[Docket No. FD 35997]

**County of Greenville, S.C.—
Acquisition Exemption—Rail Line of
Greenville County Economic
Development Corporation**

The County of Greenville, S.C. (County), a non-operating Class III rail carrier and political subdivision of the State of South Carolina, has filed a verified notice of exemption under 49

CFR 1150.41 to acquire from Greenville County Economic Development Corporation (GCEDC) approximately 3.29 miles of rail-banked line between milepost AJK 585.34 in East Greenville, S.C., and milepost AJK 588.63 in Greenville, S.C. (the Line), and to acquire GCEDC's residual common carrier obligation on the Line.¹

According to the County, it has reached an agreement with GCEDC pursuant to which, upon the effectiveness of this transaction, GCEDC will transfer to the County the entirety of its interest in the Line, including its residual common carrier obligation. The end result will be that all of GCEDC's ownership rights and responsibilities in the Line will be transferred to the County and remain rail-banked.

The County states that the proposed acquisition will not involve any provision or agreement between GCEDC and the County that would limit future interchange with a third-party connecting carrier.

The transaction may be consummated on or after March 13, 2016 (30 days after the notice of exemption was filed).

The County certifies that its projected annual revenues as a result of this transaction will not result in its becoming a Class I or Class II rail carrier and will not exceed \$5 million.

If the verified notice contains false or misleading information, the exemption is void ab initio. Petitions to revoke the exemption under 49 U.S.C. 10502(d) may be filed at any time. The filing of a petition to revoke will not automatically stay the effectiveness of the exemption. Petitions for stay must be filed no later than March 4, 2016 (at least seven days before the exemption becomes effective).

An original and 10 copies of all pleadings, referring to Docket No. FD 35997, must be filed with the Surface Transportation Board, 395 E Street SW., Washington, DC 20423-0001. In addition, a copy must be served on William A. Mullins, Baker & Miller PLLC, 2401 Pennsylvania Ave. NW., Suite 300, Washington, DC 20037.

According to the County, this action is categorically excluded from environmental review under 49 CFR 1105.6(c).

¹ The Line is rail banked pursuant to § 8(d) of the National Trails System Act, 16 U.S.C. 1247(d). See *Greenville Cty. Econ. Dev. Corp.—Aban. Exemption—in Greenville Cty, S.C.*, AB 490 (Sub-No. 2X) (STB served May 18, 2015). In a letter filed on September 14, 2015, in Docket No. AB 490 (Sub-No. 2X), the County and GCEDC jointly notified the Board that an interim trail use/rail-banking agreement had been reached between the parties. Currently, the County is the trail sponsor, and GCEDC is the owner of the Line and holder of the residual common carrier right to reactivate rail service.

Board decisions and notices are available on our Web site at “WWW.STB.DOT.GOV.”

Decided: February 23, 2016.

By the Board, Rachel D. Campbell, Director, Office of Proceedings.

Kenyatta Clay,

Clearance Clerk.

[FR Doc. 2016-04162 Filed 2-25-16; 8:45 am]

BILLING CODE 4915-01-P

SURFACE TRANSPORTATION BOARD

[Docket No. FD 35999]

**Olympia & Belmore Railroad, Inc.—
Lease and Operation Exemption
Including Interchange Commitment—
BNSF Railway Company**

Olympia & Belmore Railroad, Inc. (OBRR), a noncarrier, has filed a verified notice of exemption under 49 CFR 1150.31 to lease from BNSF Railway Company (BNSF), and to operate, approximately 13.06 miles of rail consisting of the following: (1) 5.50 miles of track between milepost 9.07 near Olympia, Wa., and milepost 14.57 near Belmore, Wa., in Thurston County, Wa.; (2) incidental overhead trackage rights over approximately 7.56 miles of Union Pacific Railroad Company track between East Olympia, Wa., and Olympia, Wa.; and (3) joint use of terminal trackage at Olympia, Wa., pursuant to a lease agreement (Agreement) dated February 12, 2016.¹

This transaction is related to a concurrently filed verified notice of exemption in *Genesee & Wyoming Inc.—Continuance in Control Exemption—Olympia & Belmore Railroad*, Docket No. FD 36000, in which Genesee & Wyoming Inc. (GWI) seeks Board approval to continue in control of OBRR under 49 CFR 1180.2(d)(2), upon OBRR's becoming a Class III rail carrier.

As required under 49 CFR 1150.43(h)(1), OBRR has disclosed in its verified notice that the subject Agreement contains an interchange commitment that affects interchange with carriers other than BNSF at the interchange point of East Olympia, Wa. OBRR has provided additional information regarding the interchange commitment as required by 49 CFR 1150.43(h).

¹ OBRR filed a confidential version of the Agreement with its notice of exemption to be kept confidential by the Board under 49 CFR 1104.14(a) without need for the filing of an accompanying motion for protective order under 49 CFR 1104.14(b). OBRR states that exhibits to the Agreement that do not relate to or affect the interchange commitment have been omitted.