

addition, non quoting firms that would like to receive the relevant information available over SQF will be allowed to connect to the SQF interface, but not send quotes.<sup>15</sup> The tiers are designed to recoup costs associated with the ports while providing increased efficiency with the new release.

The Exchange also believes that it is reasonable to eliminate the \$500 per month cap for Phlx Only Members that have 50 or less SQT assignments affiliated with member organizations because there are no members today which meet the criteria for this cap.

The Exchange believes that the amended tiers, which are increased for two categories, are equitable and not unfairly discriminatory because the features of SQF 6.0 are available to all participants. In addition, the member organizations with the greater number of ports, and therefore the greater system usage, will experience the increase.

The Exchange believes that eliminating the \$500 per month cap for the smaller organizations, defined as Phlx Only Members with 50 or less SQT assignments, is equitable and not unfairly discriminatory because there are no member organizations that will be impacted today by the elimination of this cap. There are no member organizations today that are eligible for the cap.

The Exchange believes that adopting a \$41,000 monthly cap is equitable and not unfairly discriminatory because all members utilizing SQF 6.0 ports may take advantage of the \$41,000 cap without limitation. The Exchange believes that the member organizations with the greatest number of ports will benefit from the proposed \$41,000 monthly cap. These are also the member organizations with the greatest system usage and therefore the largest costs.

Finally, the Exchange believes that it is reasonable, equitable and not unfairly discriminatory to discontinue the practice of only billing member organizations for the use of active SQF 5.0 ports to the extent the member organization was paying is paying the same (or greater) number of active SQF 6.0 ports. As mentioned herein, the Exchange believes that it has provided member organizations ample time to transition and this practice is no longer

System Event Messages (e.g., start of messages, start of system hours, start of quoting, start of opening); (4) Complex Order Strategy Auction Notifications (COLA); (5) Complex Order Strategy messages; (6) Option Trading Action Messages (e.g., halts, resumes); and (7) Complex Strategy Trading Action Message (e.g., halts, resumes).

<sup>15</sup> See Securities Exchange Act Release No. 63034 (October 4, 2010), 75 FR 62441 (October 8, 2010) (SR-Phlx-2010-124).

necessary as there should be no member organizations utilizing SQF 6.0 [sic] by January 3, 2012.

#### *B. Self-Regulatory Organization's Statement on Burden on Competition*

The Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act.

#### *C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others*

No written comments were either solicited or received

### **III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action**

The foregoing rule change has become effective pursuant to Section 19(b)(3)(A)(ii) of the Act.<sup>16</sup> At any time within 60 days of the filing of the proposed rule change, the Commission summarily may temporarily suspend such rule change if it appears to the Commission that such action is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Act. If the Commission takes such action, the Commission shall institute proceedings to determine whether the proposed rule should be approved or disapproved.

### **IV. Solicitation of Comments**

Interested persons are invited to submit written data, views, and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

#### *Electronic Comments:*

- Use the Commission's Internet comment form (<http://www.sec.gov/rules/sro.shtml>); or
- Send an email to [rule-comments@sec.gov](mailto:rule-comments@sec.gov). Please include File No. SR-Phlx-2011-157 on the subject line.

#### *Paper Comments*

- Send paper comments in triplicate to Elizabeth M. Murphy, Secretary, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-1090.

All submissions should refer to File No. SR-Phlx-2011-157. This file number should be included on the subject line if email is used. To help the

<sup>16</sup> 15 U.S.C. 78s(b)(3)(A)(ii).

Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet Web site (<http://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for Web site viewing and printing in the Commission's Public Reference Room, 100 F Street, NE., Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of such filing also will be available for inspection and copying at the principal office of the Exchange. All comments received will be posted without change; the Commission does not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly. All submissions should refer to File No. SR-Phlx-2011-157 and should be submitted on or before December 27, 2011.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.<sup>17</sup>

**Kevin M. O'Neill,**

*Deputy Secretary.*

[FR Doc. 2011-31204 Filed 12-5-11; 8:45 am]

**BILLING CODE 8011-01-P**

## **DEPARTMENT OF STATE**

[Public Notice 7709]

### **Privacy Act; System of Records: State-78, Risk Analysis and Management Records**

**SUMMARY:** Notice is hereby given that the Department of State proposes to create a system of records, Risk Analysis and Management Records, State-78, 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 January 17, 2012, unless we receive comments that will result in a contrary determination.

**ADDRESSES:** Any persons interested in commenting on the new system of

<sup>17</sup> 17 CFR 200.30-3(a)(12).

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 20522-8001.

**FOR FURTHER INFORMATION CONTACT:**

Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW.; Washington, DC 20522-8001.

**SUPPLEMENTARY INFORMATION:** The Department of State proposes that the new system will be "Risk Analysis and Management Records." The proposed system will support the vetting of directors, officers, or other employees of organizations who apply for Department of State contracts, grants, cooperative agreements, or other funding. The information collected from these organizations and individuals is specifically used to conduct screening to ensure that Department funds are not used to provide support to entities or individuals deemed to be a risk to U.S. national security interests. The records may contain criminal investigation records, investigatory material for law enforcement purposes, and confidential source information.

The Department's report was filed with the Office of Management and Budget. The new system description, Risk Analysis and Management (RAM) Records, State 78, will read as set forth below.

Dated: November 16, 2011.

**Keith D. Miller,**

*Director, Office of Operations, Bureau of Administration, U.S. Department of State.*

**STATE-78**

**SYSTEM NAME:**

Risk Analysis and Management (RAM) Records.

**SECURITY CLASSIFICATION:**

Classified and Unclassified.

**SYSTEM LOCATION:**

Department of State, 2201 C Street NW., Washington, DC 20520; other Department of State annexes, posts and missions abroad; and the United States Agency for International Development (USAID), Office of Security, 1300 Pennsylvania Avenue NW., Washington, DC 20523.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

The system covers key personnel of organizations who have applied for contracts, grants, cooperative agreements or other funding from the Department of State. These individuals may include but are not limited to principal officers or directors, program

managers, chief of party for the program, and other individuals employed by the organization.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Unclassified information in this system includes, but is not limited to: name, aliases, date and place of birth, gender (as shown in a government-issued foreign or U.S. photo ID), citizenship(s), government-issued identification information (including but not limited to Social Security number if U.S. citizen or Legal Permanent Resident, passport number, or any other numbers originated by a government that specifically identifies an individual), mailing address, telephone number(s), fax number, email address, current employer and job title. The type of grant, U.S. dollar value of contract/grant, the contract/grant start and end date, and the purpose of the contract/grant are also contained in the system.

Classified information in this system includes, but is not limited to: results generated from the screening of individuals covered by this Notice; intelligence and law enforcement information related to national security; and national security vetting and terrorism screening information provided to the Department by other agencies.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

18 U.S.C. 2339A, 2339B, 2339C; 22 U.S.C. 2151 et seq.; Executive Orders 13224, 13099 and 12947; and Homeland Security Presidential Directive-6.

**PURPOSE:**

The information in the system supports the vetting of directors, officers, or other employees of organizations who apply for Department of State contracts, grants, cooperative agreements, or other funding. The information collected from these organizations and individuals is specifically used to conduct screening to ensure that Department funds are not used to provide support to entities or individuals deemed to be a risk to U.S. national security interests.

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

Information may be disclosed to the United States Agency for International Development (USAID) and to federal government agencies for vetting programs.

The Department of State periodically publishes in the **Federal Register** its standard routine uses which apply to all of its Privacy Act systems of records. These notices appear in the form of a

Prefatory Statement. These standard routine uses apply to State-78, Risk Analysis and Management Records.

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

**STORAGE:**

Records in this system are stored in both paper and electronic format.

**RETRIEVABILITY:**

Records are retrieved by name, date and place of birth, government-issued identifying numbers (such as Social Security numbers or passport numbers), and solicitation number.

**SAFEGUARDS:**

The records are maintained in an authorized security container with access limited to authorized government personnel and authorized contractors. Physical security protections include guards and locked facilities requiring badges. Only authorized government personnel and authorized contractors can access records within the system. The Department mandates and certifies that physical and technological safeguards appropriate for classified and Sensitive but Unclassified systems are used to protect the records against unauthorized access. All authorized government personnel and authorized contractors with access to the system must hold an appropriate security clearance, sign a non-disclosure agreement, and undergo both privacy and security training.

Classified and Sensitive but Unclassified paper records are kept in an approved security container. Access to these records is limited to those authorized government personnel and authorized contractors who have a need for the records in the performance of their official duties.

Electronic records are kept in a secure database. Access to the records is restricted to those authorized government personnel and authorized contractors with a specific role in the vetting process as part of the performance of their official duties. The RAM database is housed on and accessed from a Sensitive but Unclassified computer network. Vetting requests, analyses, and results will be stored separately on a classified computer network. Both computer networks and the RAM database require a user identification name and password and approval from the Office of Security. An audit trail is maintained and periodically reviewed to monitor access to the system. When it is determined that a user no longer needs access, the user account is disabled.

Authorized government personnel and authorized contractors assigned roles in the vetting process are provided role-specific training to ensure that they are knowledgeable in how to protect personally identifiable information. Access to the Department of State records within the system will be controlled by the network firewall configuration.

Within the Department of State, all users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified 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 FSI distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to RAM 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 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.

#### RETENTION AND DISPOSAL:

Records are retired 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 the Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street, NW., Washington, DC 20522-8001.

#### SYSTEM MANAGER(S) AND ADDRESS:

Office of Risk Analysis and Management, Department of State, Washington, DC, 2201 C St. NW., Washington, DC 20520.

#### NOTIFICATION PROCEDURE:

Individuals who have cause to believe that Risk Analysis and Management Records might have records pertaining to them should write to the Director;

Office of Information Programs and Services, A/GIS/IPS, Department of State, SA-2; 515 22nd Street NW., Washington, DC 20522-8001. The individual must specify that he/she wishes the records of the Risk Analysis and Management Records to be checked. At a minimum, the individual must include: name; date and place of birth; current mailing address and zip code; signature; and the approximate dates of application for a contract, grant or other funding.

#### 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:

Information in this system is obtained from the application form completed and submitted by an organization or individual applying for a contract, grant, cooperative agreement, or other funding from the Department of State. In the case of applications submitted by an individual in his/her own capacity, the information will be collected directly from the individual applicant. Information in this system may also be obtained from public sources, agencies conducting national security screening law enforcement and intelligence agency records, and other government databases.

#### SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Pursuant to 5 U.S.C. 552a(j)(2), records in this system may be exempt from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G), (H), and (I), (e)(5) and (8), (f), (g) and (h) of the Privacy Act. Pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), records in this system may be exempt from subsections 5 U.S.C. 552a(c)(3),(d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act.

If a record contains information from other exempt systems of records, the Department of State will rely on the exemptions claimed for those systems.

[FR Doc. 2011-31270 Filed 12-5-11; 8:45 am]

BILLING CODE 4710-24-P

## DEPARTMENT OF TRANSPORTATION

### Federal Railroad Administration

[Docket Number FRA-2011-0089]

#### Petition for Waiver of Compliance

In accordance with part 211 of title 49 of the Code of Federal Regulations (CFR), this document provides the public notice that by a document dated November 9, 2011, the Association of American Railroads (AAR) and the American Short Line and Regional Railroad Association (ASLRRA) have petitioned the Federal Railroad Administration (FRA) on behalf of their members for a waiver of compliance from certain provisions of the Federal railroad safety regulations contained at 49 CFR part 231, Safety Appliance Standards. FRA assigned the petition Docket Number FRA-2011-0089.

Specifically, AAR and ASLRRA are requesting relief from section 49 CFR Section 231.27(b)(3), which requires that end platforms on boxcars be "centered on each end of car between inner ends of handholds not more than eight (8) inches above top of center sill." The AAR and ASLRRA request relief for a group of boxcars that have end platforms that may exceed the 8-inch maximum by as much as 2 inches. AAR and ASLRRA stated that more than 18,000 cars and 20 different car owners are affected. The cars were manufactured between 1977 and 2001 as provided in an attachment to the petition. AAR and ASLRRA assert that in order to correct the end platform variance, many cars would require extensive modifications that are costly and labor intensive. Additionally, AAR and ASLRRA stated that one issue is whether the cars in question actually violate 49 CFR 231.27(b)(3) based on the specific method used to measure the sill step relationship to the platform height. AAR and ASLRRA believe that waiver would resolve any end platform variance created by the ambiguous wording contained in 49 CFR 231.27(b)(3). AAR and ASLRRA also stated that they are unaware of any personal injuries or other incidents arising from the height of the end platforms. AAR and ASLRRA believe a permanent waiver would be appropriate instead of the granting of a traditional 5-year waiver.

A copy of the petition, as well as any written communications concerning the petition, is available for review online at [www.regulations.gov](http://www.regulations.gov) and in person at the U.S. Department of Transportation's (DOT) Docket Operations Facility, 1200 New Jersey Ave. SE., W12-140, Washington, DC 20590. The Docket