Proposed Rules

Federal Register

Vol. 78, No. 176

Wednesday, September 11, 2013

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 5

[Docket No. DHS–2013–0041]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security Transportation Security Administration, DHS/TSA–021, TSA Pre✓™ Application Program System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the ''Department of Homeland Security/Transportation Security Administration-021, TSA Pre✓™; Application Program System of Records'' and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before October 11, 2013.

ADDRESSES: You may submit comments, identified by docket number DHS–2013–0041, by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Peter Pietra, TSA Privacy Officer, TSA–036, 601 South 12th Street, Arlington, VA 20598–6036; or email at *TSAprivacy@dhs.gov.* For privacy questions, please contact: Jonathan R. Cantor, (202) 343–1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS)/Transportation Security Administration (TSA) proposes to establish a new DHS system of records titled, ''DHS/TSA–021 TSA Pre✓™ Application Program System of Records.''

TSA is establishing this new system of records to inform the public of the collection, maintenance, dissemination, and use of records on individuals who voluntarily submit personally identifiable information to the TSA Pre✓™ Application Program. TSA will use the information provided by applicants [1] to the Program to perform a security threat assessment to identify individuals who present a low risk to transportation security. This passenger prescreening enables TSA to determine the appropriate level of security screening the passenger will receive before the passenger receives a boarding pass.

TSA Pre✓™ Application Program. TSA Pre✓™ is a passenger prescreening initiative for low risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints.[2] TSA Pre✓™ is one of several expedited screening initiatives that TSA is implementing. TSA Pre✓™, as well as the larger set of expedited screening initiatives, enhance aviation security by permitting TSA to better focus its limited security resources on passengers who are more likely to pose a threat to civil aviation, while also facilitating and improving the commercial aviation travel experience for the public.

TSA is implementing the TSA Pre✓™ Application Program pursuant to its authority under section 109(a)(3) of the Aviation and Transportation Security Act (ATSA), Public Law 107–71 (115 Stat. 597, 613, Nov. 19, 2001, codified at 49 U.S.C. 114 note). That section authorizes TSA to ''[e]stablish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.''

Members of the public who apply to the TSA Pre✓™ Application Program will be required to pay a fee. Section 540 of the DHS Appropriations Act, 2006, Public Law 109–90 (119 Stat. 2064, 2088–89, Oct. 18, 2005), authorizes TSA to establish and collect a fee for any registered traveler program by publication of a notice in the **Federal Register**. The Department of Homeland Security will issue a separate notice of the fee for the TSA Pre✓™ Application Program in the **Federal Register**.

To apply to the TSA Pre✓™ Application Program, individuals will submit biographic and biometric information to TSA. TSA will use the information to conduct a security threat assessment of law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history records check conducted through the Federal Bureau of Investigation (FBI). The results will be used by TSA to decide if an individual poses a low risk to transportation or national security. TSA will provide individuals who meet the standards of

[1] Further information on information collection can be found in Intent To Request Approval From OMB of One New Public Collection of Information: TSA Pre✓™ Trusted Traveler Program; Republication, 78 FR 45256 (July 26, 2013) (republished for technical correction).

[2] Passengers who are eligible for expedited screening through a dedicated TSA Pre✓™ lane typically will receive more limited physical screening, *e.g.,* will be able to leave on their shoes, light outerwear, and belt, to keep their laptop in its case, and to keep their 3–1–1 compliant liquids/gels bag in a carry-on. TSA Pre✓™ lanes are available at 40 airports nationwide, with additional expansion planned. See *TSA Pre✓™ Now Available at 40 Airports Nationwide: Expedited Screening Begins at Raleigh-Durham International Airport,* http://www.tsa.gov/press/releases/2013/03/28/tsa-pre%E2%9C%93%E2%84%A2-now-available-40-airports-nationwide-expedited-screening-begins.

the security threat assessment a Known Traveler Number (KTN).[3]

The list of individuals approved under the TSA Pre✓™ Application Program, including their name, date of birth, gender, and KTN, will be provided to the TSA Secure Flight passenger prescreening system.[4] The Secure Flight system will not receive other applicant information that is maintained in the TSA Pre✓™ Application Program system of records.[5]

Eligibility for the TSA Pre✓™ Application Program is within the sole discretion of TSA, which will notify individuals who are denied eligibility in writing of the reasons for the denial. If initially deemed ineligible, applicants will have an opportunity to correct cases of misidentification or inaccurate criminal or immigration records. Consistent with 28 CFR 50.12 in cases involving criminal records, and before making a final eligibility decision, TSA will advise the applicant that the FBI criminal record discloses information that would disqualify him or her from the TSA Pre✓™ Application Program.

Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the applicant must notify TSA in writing of his or her intent to correct any information he or she believes to be inaccurate. The applicant must provide a certified revised record, or the appropriate court must forward a certified true copy of the information, prior to TSA approving eligibility of the applicant for the TSA Pre✓™ Application Program. With respect to immigration records, within 30 days after being advised that the immigration records indicate that the applicant is ineligible for the TSA Pre✓™ Application Program, the applicant must notify TSA in writing of his or her intent to correct any information believed to be inaccurate. TSA will review any information submitted and make a final decision. If neither notification nor a corrected record is received by TSA, TSA may make a final determination to deny eligibility. Individuals whom TSA determines are ineligible for the program will continue to be screened at airport security checkpoints according to TSA standard screening protocols.

To be eligible for expedited screening in a TSA Pre✓™ lane, the passenger will provide his or her KTN to the airline when making flight reservations. When the airline sends the passenger's Secure Flight Passenger Data (SFPD)[6] that includes a KTN to the Secure Flight passenger prescreening system, TSA will compare that information against the TSA Pre✓™ Application Program list (as well as watch lists) in Secure Flight before issuing an appropriate boarding pass printing instruction. If the passenger's identifying information matches the entry on the TSA Pre✓™ Application Program list, the passenger will be eligible for expedited screening, except that watch list matches will receive screening appropriate for their watch list status.

Enrollment into the TSA Pre✓™ Application Program, and use of the associated KTN, does not guarantee that an individual always will receive expedited screening at airport security checkpoints. The Program retains a component of randomness to maintain the element of unpredictability for security purposes. Accordingly, persons who have been enrolled in the TSA Pre✓™ Application Program may be randomly selected for standard physical screening on occasion. In addition, although the number of TSA Pre✓™ lanes at U.S. airports is increasing, TSA Pre✓™ is not yet available for all airports, all airlines, or all flights.

DHS Information Sharing. Consistent with DHS's information-sharing mission, TSA may share information stored in the DHS/TSA–021 TSA Pre✓™ Application Program system of records with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, TSA may share information with appropriate federal, state, local, tribal, territorial, or foreign government agencies consistent with the routine uses set forth in the system of records notice.

Notice of Proposed Rulemaking. DHS is issuing this notice of proposed rulemaking to exempt this system of records (*see* ''Exemptions claimed for this system'') from certain provisions of the Privacy Act. This newly established system will be included in DHS's inventory.

No exemption shall be asserted with respect to information maintained in the system that is submitted by a person if that person, or his or her agent, seeks access to or amendment of such information. This system, however, may contain records or information created or recompiled from information contained in other systems of records that are exempt from certain provisions of the Privacy Act. For these records or information only, as necessary and appropriate to protect such information, in accordance with 5 U.S.C. 552a(k)(1) and (k)(2), DHS also will claim the original exemptions for these records or information from the following Privacy Act (5 U.S.C. 552a) subsections: (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f). Moreover, DHS will add these exemptions to Appendix C of 6 CFR Part 5, DHS Systems of Records Exempt from the Privacy Act. Such exempt records or information may be law enforcement or national security investigation or encounter records, or terrorist screening records.

DHS needs these exemptions in order to protect information relating to investigations from disclosure to subjects of investigations and others who could interfere with investigatory material compiled for law enforcement or national security purposes. Specifically, the exemptions are required to: preclude subjects of investigations from learning of and exploiting sensitive investigatory material that would interfere with the investigative process; avoid disclosure of investigative techniques; protect sensitive and classified information compiled during the investigation; protect Transportation Security Administration Office of Intelligence and Analysis and other federal agency information; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard Sensitive Security Information pursuant to 49 U.S.C. 114(r).

Nonetheless, DHS will examine each request on a case-by-case basis and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and when it would not appear to interfere with or adversely affect the investigatory purposes of the

[3] The Known Traveler Number is a component of Secure Flight Passenger Data (SFPD), both of which are defined in the Secure Flight regulations at 49 CFR 1560.3. *See also* the Secure Flight regulations at 49 CFR Part 1560.

[4] See the Privacy Impact Assessment for the Secure Flight Program, DHS/TSA/PIA–018(e), at *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018(e).pdf. See also* the Secure Flight SORN, DHS/TSA 019, *https://www.federalregister.gov/articles/2012/11/19/2012–28058/privacy-act-of-1974-system-of-records-secure-flight-records.* The Secure Flight SORN is being updated for other reasons.

[5] This System of Records Notice does not cover all individuals who may be eligible for TSA Pre✓™ expedited screening through some other means (for example, U.S. Customs and Border Protection Global Entry members, Members of the Armed Forces). This system only covers individuals who apply to TSA for enrollment in the TSA Pre✓™ Application Program.

[6] SFPD consists of name, gender, date of birth, passport information (if available), redress number (if available), Known Traveler number (if available), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information.

systems from which the information is recompiled or in which it is contained.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/TSA–021 TSA Pre✓™ Application Program System of Records. Some information in DHS/TSA–021 TSA Pre✓™ Application Program System of Records relates to official DHS national security, immigration, and intelligence activities, and also may be Sensitive Security Information. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of investigative techniques; to ensure DHS's ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard classified information. Disclosure of information to the subject of the inquiry also could permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement or national security purposes of this system and the overall law enforcement or national security processes, the applicable exemptions may be waived on a case-by-case basis.

A notice of system of records for DHS/TSA–021 TSA Pre✓™ Application Program System of Records is also published in this issue of the **Federal Register**.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5—DISCLOSURE OF RECORDS AND INFORMATION

■ 1. The authority citation for part 5 continues to read as follows:

Authority: 6 U.S.C. 101 *et seq.;* Pub. L. 107–296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

■ 2. Amend Appendix C to Part 5 by adding paragraph 70 to read as follows:

Appendix C to Part 5—DHS Systems of Records Exempt From the Privacy Act

* * * * *

70. The DHS/TSA–021 TSA Pre✓™ Application Program System of Records consists of electronic and paper records and will be used by DHS/TSA. The DHS/TSA–021 Pre✓™ Application Program System of Records is a repository of information held by DHS on individuals who voluntarily provide personally identifiable information to the Transportation Security Administration in return for enrollment in a program that will make them eligible for expedited security screening at designated airports. This System of Records contains personally identifiable information in biographic application data, biometric information, pointer information to law enforcement databases, payment tracking, and U.S. Application membership decisions that support the TSA Pre✓™ Application Program membership decisions. The DHS/TSA–012 TSA Pre✓™ Application Program System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, territorial, or foreign government agencies.

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(k)(1) and (k)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting also would permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

Dated: September 4, 2013.

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2013–22069 Filed 9–10–13; 8:45 am]

BILLING CODE 9110–9M–P