[9110-9M-P]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

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: Final rule.

SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a newly established system of records titled, "Department of Homeland Security/Transportation Security Administration-021, TSA Pre✓™ Application Program System of Records," from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS)/Transportation Security Administration (TSA) published a Notice of Proposed Rulemaking (NPRM) in the **Federal Register,** 78 FR 55657 (Sept. 11, 2013), proposing to exempt portions of the newly established "DHS/TSA-021, TSA Pre✓™ Application Program System of Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The DHS/TSA-021 TSA Pre✓™ Application Program System of Records Notice (SORN) was published in the **Federal Register,** 78 FR 55274 (Sept. 10, 2013), and comments were invited on both the NPRM and SORN.

Public Comments

DHS received 12 comments on the NPRM and five comments on the SORN.

NPRM

Several comments exceeded the scope of the exemption rulemaking and chose instead to comment on TSA security measures. DHS/TSA will not respond to those comments.

DHS/TSA received a few comments that objected to the proposal to claim any exemptions from the Privacy Act for the release of information collected pursuant to the SORN. As stated in the NPRM, no exemption will be asserted regarding information 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. However, this system 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, such as law enforcement or national security investigation or encounter records, or terrorist screening

records. Disclosure of these records from other systems, as noted in the NPRM, could compromise investigatory material compiled for law enforcement or national security purposes. 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 systems from which the information is recompiled or in which it is contained.[1]

DHS/TSA received one comment from a private individual recommending that foreign service employees and their families be automatically included this program. The comment misapprehends the program for which the NPRM was published. The NPRM was published in association with the SORN for the TSA Pre✓™ Application program, which is designed to allow individuals to apply to be included in the program. Separately, DHS/TSA continues to evaluate populations that may otherwise be eligible for TSA Pre✓™ screening.

DHS/TSA received one comment from a private individual concerned that exemptions under the Privacy Act would allow TSA to engage in discriminatory conduct based on race and appearance, and that an individual whose application is denied would have limited recourse because TSA would not provide enough information. The security threat assessment involves recurrent checks against law enforcement, immigration, and

[1] The TSA Pre✓™ Application Program performs checks that are very similar to those performed for populations such as TSA Transportation Worker Identification Credential (TWIC) and Hazardous Material Endorsement (HME) programs. Accordingly, TSA proposed most of the same Privacy Act exemptions for the TSA Pre✓™ Application Program that are claimed for the applicable System of Records Notice for the TWIC and HME programs. The Privacy Act exemptions claimed from the Transportation Security Threat Assessment System of Records strike the right balance of permitting TWIC and HME applicants to correct errors or incomplete information in other systems of records that may affect their ability to receive one of these credentials, while also protecting sensitive law enforcement or national security information that may be included in other systems of records.

intelligence databases. TSA does not make decisions regarding eligibility for the TSA Pre✓™ Application Program based on race or appearance. 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. Individuals whom TSA determines are ineligible for the TSA Pre✓™ Application Program will continue to be screened at airport security checkpoints according to TSA standard screening protocols.

DHS/TSA received one comment from a public interest research center that asserting Privacy Act exemptions contravenes the intent of the Privacy Act. DHS does not agree that asserting exemptions provided within the Privacy Act contravenes the Privacy Act. As reflected in the OMB Privacy Act Implementation Guidelines, "the drafters of the Act recognized that application of all the requirements of the Act to certain categories of records would have had undesirable and often unacceptable effects upon agencies in the conduct of necessary public business." 40 FR 28948, 28971 (July 9, 1975).

The same commenter recognized the need to withhold information pursuant to Privacy Act exemptions during the period of the investigation, but also stated that individuals should be able to receive such information after an investigation is completed or made public, with appropriate redactions to protect the identities of witnesses and informants. This commenter stated that such post-investigation disclosures would provide individuals with the ability to address potential inaccuracies in these records, and

noted that the TSA Pre✓™ Application Program will provide applicants an opportunity to correct inaccurate or incomplete criminal records or immigration records.

As stated above, DHS will consider requests on a case-by-case basis, and in certain instances may waive applicable exemptions and release material that otherwise would be withheld. However, certain information gathered in the course of law enforcement or national security investigations or encounters, and created or recompiled from information contained in other exempt systems of records, will continue to be exempted from disclosure. Some of these records would reveal investigative techniques, sensitive security information, and classified information, or permit the subjects of investigations to interfere with related investigations. Continuing to exempt these sensitive records from disclosure is consistent with the intent and spirit of the Privacy Act. This information contained in a document qualifying for exemption does not lose its exempt status when recompiled in another record if the purposes underlying the exemption of the original document pertain to the recompilation as well.

While access under the Privacy Act may be withheld under an appropriate exemption, the DHS Traveler Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs, and has been used by individuals whose names are the same or similar to those of individuals on watch lists. See http://www.dhs.gov/dhs-trip.

SORN

DHS/TSA received five comments on the SORN. One commenter asked if TSA Pre✓™ Application Program applicants would be advised as to the reasons for a denial

of that application. As explained in the SORN and NPRM, TSA will notify applicants 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 ✓™ 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 ✓™ 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.

One advocacy group stated that records of travel itineraries should be expunged because, as the commenter claimed, they are records of how individuals exercise their First Amendment rights. The TSA Pre✓™ Application Program neither requests nor maintains applicant travel itinerary records, so this comment is inapplicable.

Contrary to some commenters' assertion that the TSA Pre✓™ Application Program infringes upon an individual's right to travel, this program will provide an added convenience to the majority of the traveling public.

A public interest research center noted that according to the SORN, Known Traveler Numbers (KTNs) will be granted to individuals who pose a "low" risk to transportation security, while the Secure Flight regulation (see 49 CFR 1560.3) provides that when a known traveler program is instituted, individuals for whom the Federal government has conducted a security threat assessment and who do "not pose a security threat" will be provided a KTN. This commenter stated that DHS thus used the SORN to amend the Secure Flight regulation. DHS disagrees that the use of these two phrases constitutes a change in the Secure Flight regulation for who may receive a KTN. In response to comments on the Secure Flight proposed rule, TSA stated that it intended "to develop and implement the Known Traveler Number as part of the Secure Flight program. . . ." and that a KTN will be assigned to individuals "for whom the Federal government has already conducted a terrorist security threat assessment and has determined does not pose a terrorist security threat." *See* 73 FR 64018, 64034 (Oct. 28, 2008).

TSA will compare TSA Pre✓™ Application Program applicants to terrorist watch lists to determine whether the individuals pose a terrorist threat, but its threat assessment also will include law enforcement records checks to determine whether applicants in other ways pose a security threat.[2] Applicants who are found to present a low risk to

[2] As TSA developed its known traveler program under the Secure Flight rule, it determined that it would require a security threat assessment similar to the threat assessment used for the TWIC and HME programs. The threat assessments for the TWIC and HME programs compare applicant names to watch lists and to law enforcement records to determine whether applicants pose a terrorist threat or other security threat. As

security, *i.e.*, they do not pose either a terrorist security threat nor a more general security threat, will be provided a KTN.[3]

The use of the phrase "low risk" is neither an expansion nor a contraction of the population that was anticipated to receive KTNs under the Secure Flight rule; rather, as the TSA Pre✓™ program was developed, the use of the term "low risk" was employed to more accurately describe who will receive a KTN. The TSA Pre✓™ Application Program is a trusted traveler program, not a program open to all except those who present a terrorist threat. This standard also is consistent with the statutory authorization TSA received from the Congress 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." See sec. 109(a)(3) of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (115 Stat. 597, 613, Nov. 19, 2001, codified at 49 U.S.C. 114 note).

TSA promulgated the Secure Flight rule under the Administrative Procedure Act (APA), 5 U.S.C. 553, and clearly indicated that TSA was still developing its KTN program. The method that TSA selected to determine who receives KTNs under the TSA Pre✓™ Application Program does not substantively affect the public to a degree sufficient to implicate the policy interests underlying notice-and-comment rulemaking

---

part of this assessment, certain criminal convictions (*e.g.*, espionage) are determined to be permanent bars to receiving a TWIC or HME, while other convictions (*e.g.*, smuggling) require a period of time to have passed post-conviction or post-imprisonment before the applicant will be considered for the program. See 49 CFR 1572.103. The TWIC and HME programs thus consider not only whether an applicant poses a terrorist threat, but also whether the applicant otherwise poses a security threat.

[3] In developing its known traveler program, TSA relied on its expertise in aviation security to determine that a "threat" includes a declaration of intent to cause harm, or something likely to cause harm. Furthermore, TSA determined that a "risk" only represents a chance of something going wrong or a possibility of danger. Therefore, TSA deemed that "low risk" individuals "do not pose a security threat" to aviation security.

requirements. As noted in the SORN, the TSA Pre✓™ Application Program does not impose any impediment on any individual traveler that is different from that experienced by the general traveling public, and individuals who TSA determines to be ineligible for the program will continue to be screened at airport security checkpoints according to TSA standard screening protocols. See 78 FR 55274, 55275. Specifically, a traveler denied admission into a TSA Pre✓™ lane because he or she does not have a KTN will face no greater screening impediment than anyone in the standard screening lane. Thus, notice-and-comment rulemaking is not required because the Secure Flight regulation notified the public that TSA would retain the ability to determine who might receive a KTN, and also because no new substantive burden or impediment for any traveler has been created. As such, the use of the phrase "low risk" does not constitute an amendment to the Secure Flight regulation.

The same commenter also suggested that TSA should make public its algorithms or thresholds for determining which TSA Pre✓™ Application Program applicants are approved. If TSA were to make its algorithms public, it would be possible for individuals who seek to disrupt civil aviation to circumvent the algorithms. Such disclosure would be contrary to TSA's mission and might endanger the flying public.

Other commenters suggested that applicant information should be destroyed immediately after providing eligible individuals a KTN. For those individuals granted KTNs, TSA will maintain the application data while the KTN is valid and for one additional year to ensure that the security mission of the agency is properly protected. Without the application data, TSA would be unable to identify instances of fraud, identity theft, evolving risks, and other security issues. Moreover, destruction of the underlying

application information will hinder TSA's ability to assist KTN holders who have lost their numbers and could cause them to have to reapply for the program. TSA also will retain application data to protect applicants' right to correct underlying information in the case of an initial denial.

Two commenters questioned whether applicant information should be shared both within and outside DHS. TSA follows standard information-sharing principles among DHS components in accordance with the Privacy Act. In addition, TSA has narrowly tailored the routine uses that it has proposed to serve its mission and promote efficiency within the Federal Government.

A public interest research center objected to three of the routine uses proposed for the system of records, arguing that the routine uses would result in blanket sharing with law enforcement agencies, foreign entities, and the public for other purposes. DHS has considered the comment but disagrees. The exercise of any routine use is subject to the requirement that sharing be compatible with the purposes for which the information was collected.

Several commenters objected that the TSA Pre✓™ Application Program violates the U.S. Constitution or international treaty. DHS disagrees with the commenters as to the Constitutionality of the program, and notes that the treaty cited by an advocacy group expressly contradicts the position taken by the commenter by excluding requirements provided by law or necessary for national security from the treaty's proscription.

After careful consideration of public comments, the Department will implement the rulemaking as proposed.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS amends 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. Add new paragraph 71 to Appendix C to Part 5 to read as follows:

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

* * * * *

71. The Department of Homeland Security (DHS)/Transportation Security Administration (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/TSA on individuals who voluntarily provide personally identifiable information (PII) to TSA in return for enrollment in a program that will make them eligible for expedited security screening at designated airports. This System of Records contains PII 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-021 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 PII 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: December 20, 2013

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

[FR Doc. 2013-31183 Filed 12/31/2013 at 8:45 am; Publication Date: 01/02/2014]