[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Part 1507

[Docket No. TSA-2007-28972]

RIN 1652-AA48

Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The Transportation Security Administration (TSA) is proposing to amend the Transportation Security regulations to exempt a new system of records from several provisions of the Privacy Act. Secure Flight Records (DHS/TSA 019) will include records used as a part of a passenger watch list matching program known as Secure Flight. The Secure Flight program implements a mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458, 118 Stat. 3638, Dec. 17, 2004) and is consistent with TSA's authority under the Aviation and Transportation Security Act (ATSA). Section 4012(a)(1) of the IRTPA requires TSA to assume from air carriers the comparison of passenger information for domestic flights to the consolidated and integrated terrorist watch list maintained by the Federal Government. Further, Section 4012(a)(2) of IRTPA similarly requires the DHS to compare passenger information for international flights to and from the United States against the consolidated and integrated terrorist watch list before departure of such flights. Under the Secure Flight program, TSA would assume the current watch list matching function

to the No Fly and Selectee from aircraft operators. TSA is proposing exemptions for DHS/TSA 019 to the extent necessary to protect the integrity of investigatory information that may be included in the system of records.

DATES: Submit comments by [Insert date 30 days after date of publication in the Federal Register.]

ADDRESSES: You may submit comments, identified by the TSA docket number to this rulemaking, using any one of the following methods:

Comments Filed Electronically: You may submit comments through the docket web site at http://dms.dot.gov. You also may submit comments through the Federal eRulemaking portal at http://www.regulations.gov.

Comments Submitted by Mail, Fax, or In Person: Address or deliver your written, signed comments to the Docket Management System at U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Ave SE, Washington, DC 20590; Fax: 202-493-2251.

See SUPPLEMENTARY INFORMATION for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: Peter Pietra, Director, Privacy Policy and Compliance, TSA-36, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; facsimile (571) 227-1400; e-mail TSAPrivacy@dhs.gov; Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528 e-mail: pia@dhs.gov.

SUPPLEMENTARY INFORMATION

Comments Invited

TSA invites interested persons to participate in this rulemaking by submitting written comments, data, or opinions. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking action. See ADDRESSES above for information on where to submit comments.

With each comment, please include your name and address, identify the docket number at the beginning of your comments, and give the reason for each comment. The most helpful comments reference a specific portion of the rulemaking, explain the reason for any recommended change, and include supporting data. You may submit comments and material electronically, in person, by mail, or fax as provided under ADDRESSES, but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in two copies, in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you want TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it to you.

TSA will file in the public docket all comments received by TSA, except for comments containing confidential information and sensitive security information.[1] TSA will consider all comments received on or before the closing date for comments and will

[1] "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Confidential or Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in FOR FURTHER INFORMATION CONTACT section.

Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold them in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA receives a request to examine or copy this information, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's (DHS') FOIA regulation found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, or advocacy group, etc.). You may review the applicable Privacy Act Statement

published in the Federal Register on April 11, 2000 (65 FR 19477), or you may visit http://dms.dot.gov.

You may review the comments in the public docket by visiting the Dockets Office between 9:00 a.m. and 5:00 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located in the West Building Ground Floor, Room W12-140, at the Department of Transportation address previously provided under ADDRESSES. Also, you may review public dockets on the Internet at http://dms.dot.gov.

Availability of Rulemaking Document

You can get an electronic copy using the Internet by--

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) web page (http://dms.dot.gov/search);

(2) Accessing the Government Printing Office's web page at http://www.gpoaccess.gov/fr/index.html; or

(3) Visiting TSA's Security Regulations web page at http://www.tsa.gov and accessing the link for "Research Center" at the top of the page.

In addition, copies are available by writing or calling the individual in the FOR FURTHER INFORMATION CONTACT section. Make sure to identify the docket number of this rulemaking.

Abbreviations and Terms Used in This Document

DHS – Department of Homeland Security

FBI – Federal Bureau of Investigation

TSA – Transportation Security Administration

Background

In order to begin the Secure Flight program, Transportation Security Administration (TSA) is publishing this Notice of Proposed Rulemaking (NPRM) to propose exemptions for DHS/TSA 019 to the extent necessary to protect the integrity of investigatory information that may be included in the system of records.

On December 17, 2004, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub.L. 108-458) was enacted. Section 4012(a) of the IRTPA directs the TSA and the Department of Homeland Security (DHS) to assume from aircraft operators the pre-flight passenger watch list matching function. TSA is carrying out this mandate through the creation of the Secure Flight program.

Section 4012(a)(1) of the IRTPA requires TSA to assume from air carriers the comparison of passenger information for domestic flights to the consolidated and integrated terrorist watch list maintained by the Federal Government. Section 4012(a)(2) of IRTPA similarly requires the DHS to compare passenger information for international flights to and from the United States against the consolidated and integrated terrorist watch list before departure of such flights. Further, as recommended by the 9/11 Commission, TSA may access the "larger set of watch lists maintained by the Federal Government."[2] Therefore, as warranted by security considerations, TSA may use the full Terrorist Screening Database (TSDB) or other government databases, such as intelligence or law enforcement databases (referred to as "watch list matching"). For example, TSA may obtain intelligence that flights flying a particular route may be subject to an increased security risk. Under this circumstance, TSA may decide to compare passenger

[2] National Commission on Terrorist Attacks Upon the Untied States, page 393.

information on some or all of the flights flying that route against the full TSDB or other government database.

TSA also is publishing in today's Federal Register a Privacy Act System of Records notice establishing a new system of records for the Secure Flight program, entitled Secure Flight Records (DHS/TSA 019). Although not required, aircraft operators may voluntarily choose to begin operational testing with TSA prior to publication of a final rule for the Secure Flight program. In the event an aircraft operator begins early operational testing with TSA, the records created as part of that testing would be included in the Secure Flight Records system and the exemptions claimed in this rulemaking would apply to such records.

The categories of records TSA will create or maintain in the course of the Secure Flight program are described in detail in the system of records notice. TSA would not assert an exemption with respect to information submitted by or on behalf of individual passengers or non-travelers in the course of making a reservation or seeking access to a secured area under the Secure Flight program. This system, however, may contain records or information recompiled from or created from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records or information only, TSA is proposing certain Privacy Act exemptions for the records contained in DHS/TSA 019 pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2), to the extent necessary to protect the integrity of watch list matching procedures performed under the Secure Flight Program.

Under 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2), an agency may exempt from certain provisions of the Privacy Act a system of records containing investigatory material

compiled for law enforcement purposes, classified information, and information pertaining to national security. The exemptions proposed here are standard law enforcement and national security exemptions exercised by a large number of federal agencies.

In the course of carrying out the Secure Flight program, TSA will review information from Federal Bureau of Investigation (FBI) systems of records and from systems of records of other law enforcement and intelligence agencies if necessary to resolve an apparent match to a Federal watch list. These may include classified and unclassified governmental terrorist, law enforcement, and intelligence databases, including databases maintained by the Department of Homeland Security, Department of Defense, National Counterterrorism Center, and FBI. Records from these systems are exempt from certain provisions of the Privacy Act because they contain law enforcement investigative information and classified information. To the extent the Secure Flight Records system relies on information from such other exempt systems of records, TSA would rely on the Privacy Act exemptions claimed for those systems.

Individuals can seek redress, in accordance with the provisions of proposed 49 CFR part 1560, subpart C, in cases where they believe they have been delayed or prohibited from boarding or denied entrance to the airport sterile area, as a result of the operation of the Secure Flight program. TSA will examine each separate request on a case-by-case basis, and after conferring with the appropriate agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public. There are no current or new information collection requirements associated with this proposed rule.

Economic Impact Analyses

This rulemaking is not a "significant regulatory action" within the meaning of Executive Order 12886. Further regulatory evaluation is not necessary because the economic impact should be minimal. Moreover, I certify that this rule would not have a significant economic impact on a substantial number of small entities, because the reporting requirements themselves are not changed and because it applies only to information on individuals.

Unfunded Mandates Assessment

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), (Pub. L. 104-4, 109 Stat. 48), requires Federal agencies to assess the effects of certain regulatory actions on State, local, and tribal governments, and the private sector. UMRA requires a written statement of economic and regulatory alternatives for proposed and final rules that contain Federal mandates. A "Federal mandate" is a new or additional enforceable duty, imposed on any State, local, or tribal government, or the private sector. If any Federal mandate causes those entities to spend, in aggregate, $100 million or more in any one year the UMRA analysis is required. This rule would not impose Federal mandates on any State, local, or tribal government or the private sector.

Executive Order 13132, Federalism

TSA has analyzed this proposed rule under the principles and criteria of Executive Order 13132, Federalism. We determined that this action would not have a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government, and therefore would not have federalism implications.

Environmental Analysis

TSA has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321-4347) and has determined that this action will not have a significant effect on the human environment.

Energy Impact Analysis

The energy impact of the notice has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Pub. L. 94-163, as amended (42 U.S.C. 6362). We

have determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects in 49 CFR Part 1507

Privacy.

The Proposed Amendments

For the reasons set forth in the preamble, the Transportation Security Administration proposes to amend part 1507 of Chapter XII of Title 49 of the Code of Federal Regulations, as follows:

PART 1507 PRIVACY ACT-EXEMPTIONS

1. The authority citation for part 1507 continues to read as follows:

Authority: 49 U.S.C. 114(l)(1), 40113, 5 U.S.C. 552a(j) and (k).

2. Add a new paragraph (k) to §1507.3 to read as follows:

§ 1507.3 Exemptions.

* * * * *

(k) *Secure Flight Records.* Secure Flight Records (DHS/TSA 019) enables TSA to maintain a system of records related to watch list matching applied to air passengers and to non-traveling individuals authorized to enter an airport sterile area. Pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2), TSA is claiming the following exemptions for certain records within the Secure Flight Records system: 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g).

In addition to records under the control of TSA, the Secure Flight system of records may include records originating from systems of records of other law enforcement and intelligence agencies which may be exempt from certain provisions of

the Privacy Act. However, TSA does not assert exemption to any provisions of the Privacy Act with respect to information submitted by or on behalf of individual passengers or non-travelers in the course of making a reservation or seeking access to a secured area under the Secure Flight program.

To the extent the Secure Flight system contains records originating from other systems of records, TSA will rely on the exemptions claimed for those records in the originating system of records. Exemptions for certain records within the Secure Flight Records system from particular subsections of the Privacy Act are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because giving a record subject access to the accounting of disclosures from records concerning him or her could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency because the individual who is the subject of the record would learn of third agency investigative interests and could take steps to evade detection or apprehension. Disclosure of the accounting also could reveal the details of watch list matching measures under the Secure Flight program, as well as capabilities and vulnerabilities of the watch list matching process, the release of which could permit an individual to evade future detection and thereby impede efforts to ensure transportation security.

(2) From subsection (c)(4) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement counterterrorism, investigatory and intelligence records. Compliance with these provisions could: alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism, law enforcement, or intelligence investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because it is not always possible for TSA or other agencies to know in advance what information is both relevant and necessary for it to complete an identity comparison between aviation passengers or certain non-travelers and a known or suspected terrorist. Also, because TSA and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it

would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3), to the extent that this subsection is interpreted to require TSA to provide notice to an individual if TSA or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsections (e)(4)(G) and (H) (Agency Requirements) and (f) (Agency Rules), because this system is exempt from the access provisions of 5 U.S.C. 552a(d).

(8) From subsection (e)(5) because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for TSA to ensure their compliance with this provision, however, TSA has implemented internal quality assurance procedures to ensure that data used in the watch list matching process is as thorough, accurate, and current as possible. In addition, in the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what

information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. However, TSA has implemented internal quality assurance procedures to ensure that the data used in the watch list matching process is as thorough, accurate, and current as possible.

(9) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on TSA and other agencies and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(10) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(11) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Issued in Arlington, Virginia on AUG 8 2007

Kip Hawley

Kip Hawley

Assistant Secretary

Hugo Teufel III

Chief Privacy Officer