DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Part 1507

[Docket No. TSA–2007–28972; Amendment No. 1507–3]

RIN 1652–AA48

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

AGENCY: Transportation Security Administration, DHS.

ACTION: Final rule.

SUMMARY: Following a Notice of Proposed Rulemaking (NPRM) and public comment, this rule amends the Transportation Security Administration (TSA)'s regulations by exempting a new system of records from several provisions of the Privacy Act. The Secure Flight Records system (DHS/TSA 019) includes records used as part of the watch list matching program known as Secure Flight, which implements a mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and is consistent with TSA's authority under the Aviation and Transportation Security Act (ATSA). Under the Secure Flight program, TSA would assume the current watch list matching function to the No Fly and Selectee Lists from aircraft operators. TSA is exempting DHS/TSA 019 from provisions of the Privacy Act to the extent necessary to protect the integrity of investigatory information that may be included in the system of records.

DATES: Effective December 10, 2007.

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;* or Hugo Teufel III (703–235–0780), Chief Privacy Officer, U.S. Department of Homeland Security, Washington, DC 20528; e-mail *pia@dhs.gov.*

SUPPLEMENTARY INFORMATION:

Availability of Rulemaking Document

You can get an electronic copy using the Internet by—

(1) Searching the electronic Federal Docket Management System (FDMS) Web page at *http://www.regulations.gov;*

(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 individuals in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires TSA to comply with small entity requests for information and advice about compliance with statutes and regulations within TSA's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in **FOR FURTHER INFORMATION CONTACT**. Persons can obtain further information regarding SBREFA on the Small Business Administration's web page at *http://www.sba.gov/advo/laws/law_lib.html.*

Abbreviations and Terms Used in This Document

DHS—Department of Homeland Security
FBI—Federal Bureau of Investigation
TSA—Transportation Security Administration

Background

The Privacy Act of 1974 (Privacy Act), 5 U.S.C. 552a, governs the means by which the U.S. Government collects, maintains, uses, and disseminates personally identifiable information. 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 the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. See 5 U.S.C. 552a(a)(5).

An individual may request access to records containing information about him or herself. 5 U.S.C. 552a(b), (d). However, the Privacy Act authorizes Government agencies to exempt systems of records from access by individuals under certain circumstances, such as where the access or disclosure of such information would impede national security or law enforcement efforts.

Exemptions from Privacy Act provisions must be established by regulation. 5 U.S.C. 552a(j), (k). TSA's Privacy Act exemptions are found at 49 CFR part 1507.

On August 23, 2007, TSA published a notice (Part III, 72 FR 48392) establishing a new Privacy Act system of records entitled Secure Flight Records (DHS/TSA 019). The Secure Flight Records system maintains records for the Secure Flight Program which carries out the requirement of section 4012(a)(1) of IRTPA (Pub. L. 08–458, 188 Stat. 3638, Dec. 17, 2004) and provides for TSA's assumption 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.'' [1] 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 information on some or all of the flights flying that route against the full TSDB or other government database.

In conjunction with the establishment and publication of the Secure Flight Records system of records on August 23, 2007, TSA initiated a proposed rulemaking (Part III, 72 FR 48397) to exempt this system of records from a number of provisions of the Privacy Act because this system of records 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, to the extent necessary to protect the integrity of watch list matching procedures performed under the Secure Flight Program and in accordance with 5 U.S.C. 552a(j)(2) 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).

Discussion of Comments

TSA received comments on the proposed rule from both the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC). Some of their comments dealt more generally with the Secure Flight Program and will be addressed in the final rule for the Secure Flight Program.

[1] ''National Commission on Terrorist Attacks Upon the United States'', page 393.

The remaining comments relate to the exemptions claimed for the Secure Flight Records system, which TSA has addressed below.

As a preliminary matter and an overall response to the comments, TSA recognizes that although there is a need for the exemptions provided for in this document, there may be instances where such exemptions can be waived. There may be times when the Privacy Act exemptions claimed here are not necessary to further a governmental interest. In appropriate circumstances, where compliance would not appear to interfere with, or adversely affect, the law enforcement and national security purposes of the system and the overall law enforcement and security process, the applicable exemptions may be waived.

1. *Applicability of Exemptions (j)(2), (k)(1), and (k)(2).* EFF raised a question about TSA's ability to use 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2) as the basis for exempting the system from portions of the Privacy Act. Exemption (j)(2) applies where a system of records consists of information compiled for purposes of a criminal investigation and the system is maintained by an agency or component of the agency that performs as its principal function any activity pertaining to the enforcement of criminal laws, including efforts to prevent, control, or reduce crime, or apprehend criminals. EFF alleges that this exemption would only apply to the Secure Flight Records system if TSA believes that millions of innocent citizens are ''criminal offenders or alleged offenders.'' TSA disagrees that the Secure Flight Records system in any way suggests that the majority of individuals undergoing screening by the Secure Flight program are criminals. However, the Secure Flight system does contain records originating from the systems of records of other law enforcement and intelligence agencies, such as records obtained from the TSC of known or suspected terrorists in the Terrorist Screening Database (TSDB) and records of individuals identified on classified and unclassified governmental watch lists, which may be properly exempt from certain provisions of the Privacy Act pursuant to (j)(2). In order to ensure that agencies' investigative or law enforcement efforts are unharmed, and information relating to DHS activities are protected from disclosure to subjects of investigations, TSA must use this exemption. However, TSA does not assert exemptions to any provision 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.

Exemption (k)(1) applies to records that contain information that have been officially classified in the interest of national security. EFF noted that the designated security classification in the Privacy Act system or records notice for Secure Flight Records is ''[u]nclassified; Sensitive Security Information'' and, therefore, this system could not be exempt under (k)(1). TSA appreciates the comment, and upon re-examination concludes that the system will not be likely to contain classified material. TSA will update its system of records notice to delete the assertion of an exemption under (k)(1).

Exemption (k)(2) applies to investigatory material compiled for law enforcement purposes that is not otherwise covered by exemption (j)(2), provided that an individual is not denied access to a record where the agency's maintenance of the record resulted in the individual being denied a right, privilege, or benefit to which he would otherwise be entitled. EFF alleges that Secure Flight potentially denies individuals their right to travel, so the exemption may not be invoked with respect to those individuals who have been denied this right and material in the system should be provided to them.

As a preliminary matter, TSA does not believe that the Secure Flight program denies individuals their right to travel. Courts have consistently held that travelers do not have a Constitutional right to travel by a single mode or the most convenient form of travel. See for example: *Town of Southold* v. *Town of East Hampton,* 477 F.3d 38, 54 (2d Cir. 2007); *Gilmore* v. *Gonzales,* 435 F.3d 1125, 1136 (9th Cir. 2006); *Miller* v. *Reed,* 176 F.3d 1202, 1205 (9th Cir. 1999). The Secure Flight program would only regulate one mode of travel (aviation), and would not impose any restriction on other mode of travel. Therefore, a restriction on an individual's ability to board an aircraft as a result of the Secure Flight program would not implicate a Constitutional right to travel.

In addition, as noted above, information in this system may be related to investigations arising out of DHS or other agency programs and activities, and may pertain to law enforcement or national security matters. In such cases, allowing access to information could alert subjects of investigations of actual or potential criminal, civil, or regulatory violations, and could reveal, in an untimely manner, DHS's and other agencies' investigative interests in law enforcement efforts to preserve national security. Further, to the extent that an individual is denied a right, benefit, or privilege due to the maintenance of a record by TSA in this system, TSA will provide access to that record to the extent the law requires.

2. *Exemption from Access and Amendment Requirements.* The bulk of both EFF and EPIC's comments constituted objections to TSA's proposal to exempt portions of the system from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(4)(G)–(I); and (f) which all relate to an individual's ability to request access to and correction of records in a system of records. Both groups are concerned that the watch lists used by the Secure Flight Program contain errors and inaccuracies that lead to inconveniences and, in some cases, a loss of liberty for individuals who are placed on a watch list in error. EFF and EPIC do not believe that TSA has an adequate redress process in place, and thus, the need for access and amendment under the Privacy Act is critical.

TSA claims these exemptions in order to protect information relating to investigations from disclosure to subjects of investigations and others who could interfere with investigatory activities. Specifically, the exemptions are required to: Prevent subjects of investigations from frustrating the investigative process; avoid disclosure of investigative techniques; protect the privacy of confidential sources; ensure TSA, DHS and other agencies ability to obtain information from third party and other sources; and safeguard sensitive information. Allowing amendment of these records could 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. The exemptions proposed here are standard law enforcement and national security exemptions exercised by Federal law enforcement and intelligence agencies.

EFF and EPIC refer to the redress process, DHS Traveler Redress Inquiry Program (DHS TRIP), as ''vague,'' ''discretionary,'' ''not meaningful,'' and ''Kafkaesque.'' These assertions are simply incorrect, and are not comments upon which TSA can meaningfully act. The DHS TRIP program is a robust and effective mechanism for individuals who believe that they have been delayed or prohibited from boarding or denied entry to the airport sterile area as the result of the Secure Flight program to

seek redress and relief. With the implementation of Secure Flight, TSA believes that it will become even more effective with uniform application by the government, rather than relying on application by individual airlines. When an individual requests access to his or her information through the redress process, the request will be examined on a case by case basis, and, after conferring with the appropriate component or agency, the agency may waive applicable exemptions in appropriate circumstances 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. Again, TSA shall not assert any exemption with respect to information submitted by and collected from the individual or the individual's representative in the course of the Secure Flight Program or any redress process associated with the underlying records.

3. *Exemption from Requirement to Collect Only Relevant and Necessary Information.* EFF and EPIC object to TSA's assertion of exemption authority under 5 U.S.C. 552a(e)(1) which permits the maintenance of information beyond that which is ''relevant and necessary'' to accomplish the agency's purpose. The groups' objection stems from their conviction that the watch lists used by Secure Flight are riddled with errors and inaccuracies. EFF states that the implementation of this exemption ''will serve only to increase the likelihood that Secure Flight will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goals of expediting the pre-boarding process for travelers and improving transportation security.'' TSA appreciates this concern and similarly seeks to ensure that data used in the watch list matching process is as thorough, accurate, and current as possible. However, TSA must exempt portions of this system from (e)(1) because it is not always possible for TSA or other agencies to know in advance what information will be relevant or necessary for it to complete an identity comparison between aviation passengers or certain non-travelers and a known or suspected terrorist. For example, for one individual hair color might be the distinguishing feature that allows TSA to distinguish him or her from someone on the watch list. For other individuals, eye color, or whether they have a tattoo may be data needed to distinguish them from someone on the watch list. For these individuals, hair or eye color is relevant, but not always necessary. In addition, 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. Further, employing this exemption is not inconsistent with the principles of the Privacy Act; the drafters of the Act established exemptions to provisions like (e)(1) to avoid inappropriately limiting the ability of the Government to carry out certain functions such as law enforcement. Constraining the collection of information in the Secure Flight Records system in accordance with the ''relevant and necessary'' requirement could discourage the appropriate collection of information and impede TSA's efforts to identify known or suspected terrorists and keep them from threatening transportation security.

4. *Exemption from Requirement of Maintaining All Records Used by the Agency in Making a Determination About an Individual with Accuracy, Relevance, Timeliness, and Completeness.* Section (e)(5) of the Privacy Act requires agencies to maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. The comments received from EFF and EPIC were concerned that the quality of the watch lists used by the Secure Flight program are mediocre, and that inaccuracies in the lists coupled with exempting records from (e)(5) will lead to a loss of convenience and even liberty for those individuals who are mistakenly put on a watch list. TSA is sensitive to these concerns, however; because many of the records in this system come from other domestic and foreign agency records systems, it is not possible for TSA to ensure compliance with (e)(5). TSA is interested in eliminating erroneous and out of date information from the watch list matching process. To that end, the agency has implemented internal quality assurance procedures to ensure that data used by Secure Flight is as complete, accurate, and current as possible. 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 reveals additional details. The restriction imposed by (e)(5) would hamper 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.

5. *Exemption from the Requirement of Judicial Review.* EFF and EPIC both object to TSA's exemption of portions of the Secure Flight system of records from 5 U.S.C. 552a(g), which grants the right to judicial review. According to EFF and EPIC, the redress process offered by TSA and DHS is ''unacceptably vague'' and ''not meaningful'' because it is too ''discretionary.'' EFF states that without the right to judicial review under the Privacy Act, it is unclear what recourse is available to an individual who has been identified as potential match through Secure Flight based on incorrect information. TSA disagrees. The redress process is effective in assisting individuals who believe they have been delayed or prohibited from boarding or denied entry to the airport sterile area, as a result of the operation of the Secure Flight program. Each separate request for redress is examined on a case by case basis, and, after conferring with the appropriate agency, the 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. If individuals disagree with the agency's final decision in the redress process, the Court of Appeals is the appropriate venue to contest the decision, not a suit for amendment of records under the Privacy Act. As courts have held, even for records that are not exempt from provisions of the Privacy Act, the Privacy Act may not be used as ''a weapon to collaterally attack agency determinations.'' *Pellerin* v. *V.A.,* 790 F.2d 1553, 1555 (11th Cir. 1986). TSA's exemption of portions of the Secure Flight Records system from judicial review does not impair an individual's ability to seek redress when they believe they have been erroneously delayed or denied boarding or entry to the airport sterile area.

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the

public and, under the provisions of PRA section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. TSA has determined that there are no current or new information collection requirements associated with this rule.

Regulatory Evaluation Summary

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.*, as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. 2531–2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

Executive Order 12866 Assessment

In conducting these analyses, TSA has determined:

1. This rulemaking is not a ''significant regulatory action'' as defined in the Executive Order. Accordingly, this rule has not been reviewed by the Office of Management and Budget (OMB). Nevertheless, TSA has reviewed this rulemaking and concluded that there will not be any significant economic impact.

2. This rulemaking would not have a significant impact on a substantial number of small entities.

3. This rulemaking would not constitute a barrier to international trade.

4. This rulemaking does not impose an unfunded mandate on state, local, or tribal governments, or on the private sector.

These analyses, available in the docket, are summarized below.

Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) of 1980 requires that agencies perform a review to determine whether a proposed or final rule will have a significant economic impact on a substantial number of small entities. If the determination is that it will, the agency must prepare a regulatory flexibility analysis as described in the RFA. For purposes of the RFA, small entities include small businesses, not-for-profit organizations, and small governmental jurisdictions. Individuals and States are not included in the definition of a small entity.

This final rule exempts records in the Secure Flight Records system of records from certain provisions of the Privacy Act. TSA certifies that this rulemaking will not have a significant economic impact on a substantial number of small entities. Further, the exemptions to the Privacy Act apply to individuals, and individuals are not covered entities under the RFA.

International Trade Impact Assessment

This rulemaking will not constitute a barrier to international trade. The exemptions relate to criminal investigations and agency documentation and, therefore, do not create any new costs or barriers to trade.

Executive Order 13132, Federalism

TSA has analyzed this final rule under the principles and criteria of Executive Order 13132, Federalism. We determined that this action will not have a substantial direct effect on the States, or 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, does 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

The energy impact of the action has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Public Law 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 Amendments

■ In consideration of the foregoing, the Transportation Security Administration amends part 1507 of Chapter XII, 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.* (1) 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) 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).

(2) 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.

(3) 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:

(i) 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.

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

(iii) 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.

(iv) 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. In addition, 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.

(v) 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.

(vi) 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.

(vii) 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).

(viii) 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.

(ix) 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.

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

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

Issued in Arlington, Virginia, on November 2, 2007.

Kip Hawley,

Assistant Secretary, Transportation Security Administration.

John Kropf,

Deputy Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E7–21907 Filed 11–8–07; 8:45 am]

BILLING CODE 9110–05–P