

requirements of filing a reexamination before a filing date will be assigned to a reexamination. Interested persons are requested to send comments regarding these information collections, including suggestions for reducing this burden to: (1) The Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10202, 725 17th Street, NW., Washington, DC 20503, Attention: Desk Officer for the Patent and Trademark Office; and (2) Robert J. Spar, Director, Office of Patent Legal Administration, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Notwithstanding any other provision of law, no person is required to respond to, nor shall a person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB control number.

#### List of Subjects in 37 CFR Part 1

Administrative practice and procedure, Courts, Freedom of information, Inventions and patents, Reporting and recordkeeping requirements, Small businesses, and Biologics.

■ For the reasons set forth in the preamble, the interim rule amending 37 CFR part 1 which was published at 71 FR 9260-62 on February 23, 2006, is adopted as final with the following changes:

#### PART 1—RULES OF PRACTICE IN PATENT CASES

■ 1. The authority citation for 37 CFR part 1 continues to read as follows:

**Authority:** 35 U.S.C. 2(b)(2), unless otherwise noted.

■ 2. Section 1.11 is amended by revising paragraph (c) to read as follows:

##### § 1.11 Files open to the public.

\* \* \* \* \*

(c) All requests for reexamination for which all the requirements of § 1.510 or § 1.915 have been satisfied will be announced in the *Official Gazette*. Any reexaminations at the initiative of the Director pursuant to § 1.520 will also be announced in the *Official Gazette*. The announcement shall include at least the date of the request, if any, the reexamination request control number or the Director initiated order control number, patent number, title, class and subclass, name of the inventor, name of the patent owner of record, and the

examining group to which the reexamination is assigned.

\* \* \* \* \*

■ 3. Section 1.510 is amended by revising paragraphs (c) and (d) to read as follows:

##### § 1.510 Request for *ex parte* reexamination.

\* \* \* \* \*

(c) If the request does not include the fee for requesting *ex parte* reexamination required by paragraph (a) of this section and meet all the requirements by paragraph (b) of this section, then the person identified as requesting reexamination will be so notified and will generally be given an opportunity to complete the request within a specified time. Failure to comply with the notice will result in the *ex parte* reexamination request not being granted a filing date, and will result in placement of the request in the patent file as a citation if it complies with the requirements of § 1.501.

(d) The filing date of the request for *ex parte* reexamination is the date on which the request satisfies all the requirements of this section.

\* \* \* \* \*

■ 4. Section 1.915 is amended by revising paragraph (d) to read as follows:

##### § 1.915 Content of request for *inter partes* reexamination.

\* \* \* \* \*

(d) If the *inter partes* request does not include the fee for requesting *inter partes* reexamination required by paragraph (a) of this section and meet all the requirements of paragraph (b) of this section, then the person identified as requesting *inter partes* reexamination will be so notified and will generally be given an opportunity to complete the request within a specified time. Failure to comply with the notice will result in the *inter partes* reexamination request not being granted a filing date, and will result in placement of the request in the patent file as a citation if it complies with the requirements of § 1.501.

Dated: July 31, 2006.

Jon W. Dudas,

*Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.*

[FR Doc. E6-12600 Filed 8-3-06; 8:45 am]

BILLING CODE 3510-16-P

## DEPARTMENT OF HOMELAND SECURITY

### Transportation Security Administration

#### 49 CFR Part 1507

[Docket No. TSA-2004-19845; Amendment No. 1507-2]

RIN 1652-AA34

### Privacy Act of 1974: Implementation of Exemptions; Intelligence, Enforcement, Internal Investigation, and Background Investigation Records

**AGENCY:** Transportation Security Administration, DHS.

**ACTION:** Final rule.

**SUMMARY:** The Transportation Security Administration is amending its regulations to exempt four systems of records from certain provisions of the Privacy Act. The systems intended for exemption are the Transportation Security Intelligence Service Operations Files, the Personnel Background Investigation File System, the Transportation Security Enforcement Record System, and the Internal Investigation Record.

**DATES:** Effective September 5, 2006.

**FOR FURTHER INFORMATION CONTACT:** Lisa S. Dean, Privacy Officer, Office of Transportation Security Policy, TSA-9, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; telephone (571) 227-3947; facsimile (571) 227-2555.

#### SUPPLEMENTARY INFORMATION:

##### 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.

##### Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires the Transportation Security Administration (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](http://www.sba.gov/advo/laws/law_lib.html).

## I. Analysis of the Final Rule

### A. 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. For example, allowing the subject of an ongoing law enforcement investigation to access his or her investigative file could impede the investigation or allow the subject to avoid detection or apprehension.

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.

### B. Amendments to TSA's Privacy Act Exemptions

On December 10, 2004, TSA published a notice of proposed rulemaking in the **Federal Register** (69 FR 71767) seeking to exempt four systems of records from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k). The four systems of records are:

(1) The Transportation Security Intelligence Service (TSIS) Operations Files (DHS/TSA 011), under which TSA maintains records on intelligence, counterintelligence, transportation security, and information systems security matters as they relate to TSA's mission of protecting the nation's transportation systems;

(2) The Personnel Background Investigation File System (PBIFS) (DHS/TSA 004), under which TSA maintains investigative and background records used to make suitability and eligibility determinations for employment;

(3) The Transportation Security Enforcement Record System (TSERS) (DHS/TSA 001), which serves as an enforcement docket system; and

(4) The Internal Investigation Record System (IIRS) (DHS/TSA 005), under which TSA maintains records that facilitate the management of investigations into allegations or appearances of misconduct by current and former TSA employees or contractors and investigations of security-related incidents and reviews of TSA programs and operations.

In the December 10, 2004 notice of proposed rulemaking, TSA proposed to add 5 U.S.C. 552a(k)(1)<sup>1</sup> as an authority to exempt the Personnel Background Investigation File System (DHS/TSA 004) from the exemptions previously established for this system. See 49 CFR 1507.3. TSA also proposed to add 5 U.S.C. 552a(j)(2) (a general law enforcement exemption) as an authority to exempt the Transportation Security Enforcement Record System (DHS/TSA 001) and the Internal Investigation Record System (DHS/TSA 005) from the provisions previously claimed for those two systems, and to now include an exemption for those two systems of records from subsection (e)(3) of the Privacy Act.<sup>2</sup>

This final rule adopts the proposed rule with only two technical changes from the proposed rule. First, TSA changed references to "security sensitive information" to read "sensitive security information." Second, TSA revised § 1507.3(j)(1) (Accounting for Disclosures) to add text inadvertently omitted from the proposed rule related to the possibility that release of the accounting of disclosures could "reveal investigative interest on the part of the Transportation Security Administration, as well as the recipient." The proposed rule stated that release of the accounting of disclosures could "alert the subject of

<sup>1</sup> Section 552a(k)(1) authorizes the application of exemption (b)(1) under the Freedom of Information Act (5 U.S.C. 552) protecting from disclosure "matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy" and that are properly classified under such Executive Order.

<sup>2</sup> Section 552a(e)(3) requires the agency collecting information from an individual to inform the individual of the authority for the agency to collect the information, the purpose and intended routine uses of such information, and the potential effects on the individual if the information requested is not provided to the Government.

intelligence gathering operations on the part of the Transportation Security Administration as well as the recipient." This implied that TSA engages in intelligence gathering operations, which is not the case. TSA is a recipient of intelligence information and engages in analysis and dissemination of that information. The addition of the language described above corrects this incorrect implication and is consistent with the language used in the justification for exemption in § 1507.3(j)(2) (Access to Records).

### C. Response to Public Comments

TSA received two letters commenting on the proposed rule and one comment encouraging TSA to establish redress procedures whereby air carrier customers can report and correct any inaccurate information they believe TSA possesses. TSA received consolidated comments on the proposed rule from the Electronic Frontier Foundation, PrivacyActivism, Privacy Rights Clearinghouse, the Fairfax County Privacy Council, and the World Privacy Forum (collectively, Privacy Groups). TSA also received comments from the Owner-Operator Independent Drivers Association, Inc. (OOIDA). A number of the comments from the Privacy Groups relate to the scope and routine uses for the Transportation Security Enforcement Record System (TSERS) (DHS/TSA 001) and the Transportation Security Intelligence Service (TSIS) Operations Files (DHS/TSA 011). The remaining comments relate to the exemptions claimed for these systems, 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 application of 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 purposes of this system and the overall law enforcement process, the applicable exemptions may be waived.

#### 1. Applicability of TSERS and TSIS

OOIDA requests clarification as to whether TSERS (DHS/TSA 001) and TSIS (DHS/TSA 011) apply to records TSA maintains in conjunction with conducting threat assessments of commercial truck drivers applying for hazardous materials (hazmat) endorsements. OOIDA expresses concern that the exemptions and routine

uses applicable to these two records systems are inconsistent with certain protections for hazmat drivers envisioned by the regulation governing threat assessments for those drivers.

TSA notes that records relating to threat assessments for hazmat drivers are contained within the Transportation Security Threat Assessment System (T-STAS) DHS/TSA 002, and are not automatically included in TSERS or TSIS. A driver's records may become a part of TSERS, only if the driver is involved in a violation or potential violation of law.

## 2. Exemption From Requirement To Give an Accounting for Disclosures

The Privacy Groups object to TSA's proposal to exempt TSERS (DHS/TSA 001) and TSIS (DHS/TSA 011) from the requirement in 5 U.S.C. 552a(c)(3) to furnish individuals with an accounting for disclosures of records. They state that this exemption is not necessary because disclosures for civil and criminal law enforcement activity already are exempt from the disclosure requirements in 5 U.S.C. 552a(c)(3). See 5 U.S.C. 552a(c)(3) and (b)(7).

TSA notes that disclosures pursuant to subsection (b)(7) of the Privacy Act are not the only disclosures TSA may need to make from these systems. TSA may need to make a disclosure, for instance, when the agency merely suspects a violation of law. Accounting of such a disclosure would not be exempted under 5 U.S.C. 552a(c)(3) and (b)(7), because that limited exemption applies only where the disclosure results from a written request from any agency head specifying the particular portion of the record desired. The current routine uses applicable to the TSERS and TSIS systems of records permit disclosure of information in those systems to Federal, State, local, tribal, territorial, foreign or international agencies responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation. Any requirement to disclose the accounting of disclosures compiled under the requirements of 5 U.S.C. 552(a)(c)(3) may interfere with a law enforcement investigation, particularly if the subject of the investigation is unaware of the investigation. Consequently, TSA must assert an exemption from the accounting requirements of 5 U.S.C. 552a(c)(3) generally.

TSA notes that the ability to use a routine use for certain disclosures was intended as an addition to the type of

disclosures for civil or criminal law enforcement activity under 5 U.S.C. 552a(b)(7). See Office of Management and Budget Guidance, 40 FR 28955 (July 9, 1975). Dependence on the disclosure authority in subsection (b)(7) for all investigations, therefore, is not appropriate, and must be supplemented by routine uses. For this reason, TSA also is claiming an exemption from 5 U.S.C. 552a(c)(3), generally, to cover access to the accounting of the disclosures made pursuant to these routine uses.

As explained in this document, TSA is exempting the two systems of records, TSERS (DHS/TSA 001) and TSIS (DHS/TSA 011), from the accounting for disclosures in order to protect the integrity of investigations. Notifying individuals of an investigation alerts those individuals who are subject to the investigation, and could help them evade investigation and compromise security. Both of the systems of records at issue are essential to TSA's transportation security mission.

TSA notes that with respect to TSERS (DHS/TSA 001), this rulemaking only adds 5 U.S.C. 552a(j)(2) as an authority for exemptions, and that TSA previously published a final rule on June 25, 2004 (69 FR 35536), exempting the TSERS (DHS/TSA 001) system from the accounting, access, and relevance/necessity requirements. TSERS is a system intended to cover civil and criminal enforcement and inspection records, and records related to investigations or prosecution of violations or potential violations of law. TSERS records are also used to record details of security-related activity, such as passenger or baggage screening, and include suspicious activity reports. TSIS is a system intended to cover records on intelligence, counterintelligence, transportation security, and information security matters as they relate to TSA's mission of protecting the nation's transportation systems. TSIS records also are used to identify potential threats to transportation security, uphold and enforce the law, and ensure public safety. Both TSERS and TSIS contain records that are investigatory in nature. If TSA is investigating a security incident, or the security activities of a regulated entity, it is imperative that the individuals involved not be given the opportunity to evade detection and resulting enforcement action. Providing this knowledge to such individuals defeats the investigation.

Commenters suggest that an exemption from the requirement to provide individuals access to the accounting of disclosures would prevent an individual wrongly denied a job,

contract, or license from learning to whom incorrect information had been disclosed, and from attempting to correct any error.

However, because the focus of the TSERS and TSIS systems is to support transportation security and the use of appropriate investigatory authority, TSA must be able to notify transportation employers about their employees that violate TSA regulations or are determined to pose a threat to transportation, particularly if the investigation requires the cooperation of the employer. Where an employer takes action against an individual, it is expected that the employer will likely notify the individual of the basis of the action, including the fact of a disclosure from TSA. So, for example, if an air carrier employee is caught with a firearm at a screening checkpoint, TSA will report that incident to the air carrier for its consideration in connection with revoking the employee's security credentials. The air carrier will likely notify the individual of the basis of the revocation. The individual can contest the Notice of Violation from TSA, or can seek redress under the procedures outlined in the applicable Privacy Impact Assessment. If, on the other hand, TSA is investigating an air carrier employee for on-going access door violations, TSA might notify the employer of the investigation, but ask that the employer not notify the employee of the disclosure in order to preserve the investigation. In developing these systems, TSA has attempted to strike a balance between the agency's mission to protect the nation against threats to transportation, and the privacy and civil liberties of the public.

## 3. Exemption From Requirement To Collect Only Relevant and Necessary Information

The Privacy Groups also 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 Privacy Groups state that the assertion of this exemption would lead to the wide dissemination of irrelevant and inaccurate information.

While the commenters focus on the relevance requirement, they fail to address the necessity component of the statute. The necessity of maintaining a particular piece of information often is difficult to determine in the context of an investigation, particularly in its nascent stages. TSA will, of course, collect information that it deems relevant to the investigation as

collection of irrelevant information wastes scarce resources, is inefficient, and uses database space inappropriately. It is, however, not always possible to determine the relevance *and* necessity (emphasis added) of specific information early in the investigative process. TSA should not be required to discard relevant information as unnecessary when such information may very well turn out to be necessary later in an investigation.

To ensure that no key pieces of information are lost, and in the interest of protecting the integrity of investigations, TSA is claiming an exemption from the relevancy and necessity requirements. TSERS and TSIS are both systems crucial to the TSA's transportation security mission. Without this exemption, TSA's ability to conduct thorough investigations, and ultimately its ability to protect transportation security, is jeopardized. As to the allegation that inaccurate and irrelevant information will be "widely" disseminated, TSA disseminates information only as appropriate and authorized under the Privacy Act.

#### 4. Exemption From Notice Requirements

Finally, the Privacy Groups object to TSA's proposed exemption of TSERS (DHS/TSA 001) from the requirement of 5 U.S.C. 552a(e)(3), which requires that, prior to requiring an individual to submit information to an agency, the agency provide notice of the authority under which information is collected, the purpose for which it is intended to be used, routine uses which may be made; and the consequences to the individual for refusing to provide the information. TSA claims this exemption in order to safeguard the integrity of investigations. Early notice to all individuals of the authority, voluntary nature, purpose, and routine uses of the information collected would impair investigations into transportation security. It would reveal TSA's investigative interest in the individual, as well as the nature of the investigation, thereby providing the individual an opportunity to interfere with the investigation or evade detection or suspicion.

Also, the Privacy Groups state that this exemption should not apply to information that individuals provide to TSA for purposes of passenger screening. With respect to the Privacy Groups' concerns regarding passenger reservations data, such information will be part of a separate system of records to be published in connection with the Secure Flight Program. The TSERS (DHS/TSA 001) system does not cover

the records TSA will maintain for the operation of the Secure Flight Program.

The Air Transport Association of America, Inc, has no comments on the proposed rule, but encourages TSA to establish redress procedures whereby air carrier customers can report and correct any inaccurate information they believe TSA possesses. TSA has established an Office of Transportation Security Redress that will be the public's point of contact for this purpose. TSA also will publish a system of records notice for the Secure Flight program that will be the primary system affecting passengers.

## II. Regulatory Requirements

### A. Regulatory Impact Analyses

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).

In conducting these analyses, TSA has determined:

#### 1. Executive Order 12866 Assessment

This rule is a significant regulatory action under section 3(f) of Executive Order 12866, "Regulatory Planning and Review," 58 FR 51735 (Oct. 4, 1993) (as amended). Accordingly, this rule has been reviewed by the Office of Management and Budget (OMB). Distilled to its essence, this rulemaking exempts TSA from providing a privacy act notice in the context of criminal investigations, permits TSA to withhold classified documents from employees seeking their background investigation, and exempts TSA intelligence records

from access, accounting, and relevance/necessity requirements as outlined elsewhere in this rulemaking. TSA's ability to perform law enforcement and intelligence functions connected to transportation security are significantly degraded without these exemptions.

#### 2. Regulatory Flexibility Act Assessment

The Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), as amended by the Small Business Regulatory Enforcement and Fairness Act of 1996 (SBREFA), requires an agency to prepare and make available to the public a regulatory flexibility analysis that describes the effect of the rule on small entities (i.e., small businesses, small organizations, and small governmental jurisdictions). Section 605 of the RFA allows an agency, in lieu of preparing an analysis, to certify that a rule is not expected to have a significant economic impact on a substantial number of small entities. Accordingly, TSA certifies that this final rule will not have a significant impact on a substantial number of small entities. The final rule imposes no duties or obligations on small entities. This rule provides exemptions to existing procedures and adds no new regulated parties. Further, the exemptions to the Privacy Act apply to individuals, and individuals are not covered entities under the RFA.

#### 3. 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.

#### 4. 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 rulemaking will not impose an unfunded mandate on state, local, or tribal governments, or on the private sector. This rule will provide exemptions rather than new requirements. The exemptions relate to

criminal investigations of individuals and agency documentation and, therefore, do not create any new requirements for state, local, or tribal governments, or on the private sector.

#### B. 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.

#### C. Executive Order 13132, Federalism

TSA has analyzed this rule under the principles and criteria of Executive Order 13132, Federalism. This action will 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 will not have federalism implications.

#### D. 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.

#### E. Energy Impact

The energy impact of this 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). This rulemaking is not a major regulatory action under the provisions of the EPCA.

#### List of Subjects in 49 CFR Part 1507

Privacy.

#### The Amendment

■ 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. Amend § 1507.3 by revising paragraphs (a), (c), and (d), and by adding a new paragraph (j) to read as follows:

#### § 1507.3 Exemptions.

\* \* \* \* \*

(a) *Transportation Security Enforcement Record System (DHS/TSA 001)*. The Transportation Security Enforcement Record System (TSERS) (DHS/TSA 001) enables TSA to maintain a system of records related to the screening of passengers and property and they may be used to identify, review, analyze, investigate, and prosecute violations or potential violations of criminal statutes and transportation security laws. Pursuant to exemptions (j)(2), (k)(1), and (k)(2) of the Privacy Act, DHS/TSA 001 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(3), (e)(4)(G), (H), and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) 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 the investigation and reveal investigative interest on the part of TSA, as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to transportation security, law enforcement efforts, and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system.

(2) 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 the investigation and reveal investigative interest on the part of TSA, as well as the recipient agency. Access to the records would permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records would interfere with ongoing investigations and law enforcement activities, and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting

access and amendment to such information also could disclose sensitive security information, which could be detrimental to transportation security.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of transportation security laws, 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 enforcement of transportation security laws, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(4) From subsection (e)(3) (Privacy Act Statement) because disclosing the authority, purpose, routine uses, and potential consequences of not providing information could reveal the investigative interests of TSA, as well as the nature and scope of an investigation, the disclosure of which could enable individuals to circumvent agency regulations or statutes.

(5) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

\* \* \* \* \*

(c) *Personnel Background Investigation File System (DHS/TSA 004)*. The Personnel Background Investigation File System (PBIFS) (DHS/TSA 004) enables TSA to maintain investigative and background material used to make suitability and eligibility determinations regarding current and former TSA employees, applicants for TSA employment, and TSA contract employees. Pursuant to exemptions (k)(1) and (k)(5) of the Privacy Act, the Personnel Background Investigation File System is exempt from 5 U.S.C. 552a(c)(3) (Accounting of Disclosures) and (d) (Access to Records). Exemptions from the particular subsections are justified because this system contains investigatory material compiled solely for determining suitability, eligibility, and qualifications for Federal civilian employment. To the extent that the disclosure of material would reveal any classified material or the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence, the applicability of exemption (k)(5) will be required to honor promises of

confidentiality should the data subject request access to or amendment of the record, or access to the accounting of disclosures of the record. Exemption (k)(1) will be required to protect any classified information that may be in this system.

(d) *Internal Investigation Record System (DHS/TSA 005)*. The Internal Investigation Record System (IIRS) (DHS/TSA 005) contains records of internal investigations for all modes of transportation for which TSA has security-related duties. This system covers information regarding investigations of allegations or appearances of misconduct of current or former TSA employees or contractors and provides support for any adverse action that may occur as a result of the findings of the investigation. It is being modified to cover investigations of security-related incidents and reviews of TSA programs and operations. Pursuant to exemptions (j)(2), (k)(1), and (k)(2) of the Privacy Act, DHS/TSA 005 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(3), (e)(4)(G), (H), and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures 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, as the individual who is the subject of a record would learn of third-agency investigative interests and thereby avoid detection or apprehension, as well as to TSA investigative efforts.

(2) From subsection (d) (Access to Records) because access to the records contained in this system could reveal investigative techniques and procedures of the investigators, as well as the nature and scope of the investigation, the disclosure of which could enable individuals to circumvent agency regulations or statutes. The information contained in the system might include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such records could reveal sensitive security information protected pursuant to 49 U.S.C. 114(s), the disclosure of which could be detrimental to the security of transportation.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because

third agency records obtained or made available to TSA during the course of an investigation may occasionally contain information that is not strictly relevant or necessary to a specific investigation. In the interests of administering an effective and comprehensive investigation program, it is appropriate and necessary for TSA to retain all such information that may aid in that process.

(4) From subsection (e)(3) (Privacy Act Statement) because disclosing the authority, purpose, routine uses, and potential consequences of not providing information could reveal the targets of interests of the investigating office, as well as the nature and scope of an investigation, the disclosure of which could enable individuals to circumvent agency regulations or statutes.

(5) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

\* \* \* \* \*

(j) *Transportation Security Intelligence Service (TSIS) Operations Files*. Transportation Security Intelligence Service Operations Files (TSIS) (DHS/TSA 011) enables TSA to maintain a system of records related to intelligence gathering activities used to identify, review, analyze, investigate, and prevent violations or potential violations of transportation security laws. This system also contains records relating to determinations about individuals' qualifications, eligibility, or suitability for access to classified information. Pursuant to exemptions (j)(2), (k)(1), (k)(2), and (k)(5) of the Privacy Act, DHS/TSA 011 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f). Exemptions from particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of intelligence gather operations and reveal investigative interest on the part of the Transportation Security Administration, as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to transportation security law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede operations and avoid detection and apprehension, which undermined the entire system. Disclosure of the accounting may also reveal the existence of information that

is classified or sensitive security information, the release of which would be detrimental to the security of transportation.

(2) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of intelligence gathering operations and reveal investigative interest on the part of the Transportation Security Administration. Access to the records would permit the individual who is the subject of a record to impede operations and possibly avoid detection or apprehension. Amendment of the records would interfere with ongoing intelligence and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continually reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose sensitive security information, which could be detrimental to transportation security if released. This system may also include information necessary to make a determination as to an individual's qualifications, eligibility, or suitability for access to classified information, the release of which would reveal the identity of a source who received an express or implied assurance that their identity would not be revealed to the subject of the record.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of gathering and analyzing information about potential threats to transportation security, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific operation. In the interests of transportation security, it is appropriate to retain all information that may aid in identifying threats to transportation security and establishing other patterns of unlawful activity.

(4) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access and amendment provisions of subsection (d).

Issued in Arlington, Virginia, on July 28, 2006.

**Kip Hawley,**

*Assistant Secretary.*

[FR Doc. 06-6670 Filed 8-3-06; 8:45 am]

BILLING CODE 9110-05-P