(56 FR 35952, July 29, 1991). Health care providers and others may voluntarily seek to comply with these provisions so that they have the assurance that their business practices will not be subject to any enforcement action under the anti-kickback statute or related administrative authorities.

To date, OIG has developed and codified in 42 CFR 1001.952 a total of 22 final safe harbors that describe practices that are sheltered from liability.

B. OIG Special Fraud Alerts

The OIG has also periodically issued Special Fraud Alerts to give continuing guidance to health care providers with respect to practices OIG finds potentially fraudulent or abusive. The Special Fraud Alerts encourage industry compliance by giving providers guidance that can be applied to their own practices. The OIG Special Fraud Alerts are intended for extensive distribution directly to the health care provider community, as well as to those charged with administering the Federal health care programs.

In developing these Special Fraud Alerts, OIG has relied on a number of sources and has consulted directly with experts in the subject field, including those within OIG, other agencies of the Department, other Federal and State agencies, and those in the health care industry. To date, OIG has issued 12 individual Special Fraud Alerts.

C. Section 205 of Public Law 104–191

Section 205 of Public Law 104–191 requires the Department to develop and publish an annual notice in the **Federal Register** formally soliciting proposals for modifying existing safe harbors to the anti-kickback statute and for developing new safe harbors and Special Fraud Alerts.

In developing safe harbors for a criminal statute, OIG is required to engage in a thorough review of the range of factual circumstances that may fall within the proposed safe harbor subject area so as to uncover potential opportunities for fraud and abuse. Only then can OIG determine, in consultation with the Department of Justice, whether it can effectively develop regulatory limitations and controls that will permit beneficial and innocuous arrangements within a subject area while, at the same time, protecting the Federal health care programs and their beneficiaries from abusive practices.

II. Solicitation of Additional New Recommendations and Proposals

In accordance with the requirements of section 205 of Public Law 104–191, OIG last published a **Federal Register** solicitation notice for developing new safe harbors and Special Fraud Alerts on December 12, 2003 (68 FR 69366). As required under section 205, a status report of the public comments received in response to that notice is set forth in Appendix G to the OIG's Semiannual Report covering the period April 1, 2004 through September, 30, 2004.[1] The OIG is not seeking additional public comment on the proposals listed in Appendix G at this time. Rather, this notice seeks additional recommendations regarding the development of proposed or modified safe harbor regulations and new Special Fraud Alerts beyond those summarized in Appendix G to the OIG Semiannual Report referenced above.

Criteria for Modifying and Establishing Safe Harbor Provisions

In accordance with section 205 of HIPAA, we will consider a number of factors in reviewing proposals for new or modified safe harbor provisions, such as the extent to which the proposals would affect an increase or decrease in—

- Access to health care services;
- The quality of services;
- Patient freedom of choice among health care providers;
- Competition among health care providers;
- The cost to Federal health care programs;
- The potential overutilization of the health care services; and
- The ability of health care facilities to provide services in medically underserved areas or to medically underserved populations.

In addition, we will also take into consideration other factors, including, for example, the existence (or nonexistence) of any potential financial benefit to health care professionals or providers that may take into account their decisions whether to (1) order a health care item or service, or (2) arrange for a referral of health care items or services to a particular practitioner or provider.

Criteria for Developing Special Fraud Alerts

In determining whether to issue additional Special Fraud Alerts, we will also consider whether, and to what extent, the practices that would be identified in a new Special Fraud Alert may result in any of the consequences set forth above, as well as the volume and frequency of the conduct that would be identified in the Special Fraud Alert.

A detailed explanation of justifications for, or empirical data supporting, a suggestion for a safe harbor or Special Fraud Alert would be helpful and should, if possible, be included in any response to this solicitation.

Dated: November 24, 2004.

Daniel R. Levinson,

Acting Inspector General.

[FR Doc. 04–27117 Filed 12–9–04; 8:45 am]

BILLING CODE 4150–04–P

[1] The OIG Semiannual Report can be accessed through the OIG Web site at *http://oig.hhs.gov/publications/semiannual.html.*

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Part 1507

[Docket No. TSA–2004–19845]

RIN 1652–AA34

Privacy Act of 1974: Implementation of Exemptions

AGENCY: Transportation Security Administration (TSA), DHS.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: TSA proposes to exempt Transportation Security Intelligence Service (TSIS) Operations Files (DHS/TSA 011) from several provisions of the Privacy Act; to add 5 U.S.C. 552a(k)(1) as an authority to exempt the Personnel Background Investigation File System (DHS/TSA 004) from the provisions previously claimed for that system; and to add 5 U.S.C. 552a(j)(2) 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, to now include subsection (e)(3). Public comment is invited.

DATES: Submit comments by January 10, 2005.

ADDRESSES: You must identify the TSA docket number when you submit comments 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.* 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, 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 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, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590–0001; Fax: 202–493–2251.

Reviewing Comments in the Docket: You may review the public docket containing comments in person in the Dockets Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located on the plaza level of the NASSIF Building at the Department of Transportation address above. Also, you may review public dockets on the Internet at *http://dms.dot.gov.*

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

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

SUPPLEMENTARY INFORMATION:

Comments Invited

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

With each comment, please include your name and address, identify the docket number TSA–2004–19845 at the beginning of your comments, and give the reason for each comment. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. You may submit comments and material electronically, in person, or by mail 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 the TSA to acknowledge receipt of your comments on this rulemaking, 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.

Except for comments containing confidential information and SSI, we will file in the public docket all comments we receive, as well as a report summarizing each substantive public contact with TSA personnel concerning this rulemaking. The docket is available for public inspection before and after the comment closing date.

We will consider all comments we receive on or before the closing date for comments. We will consider comments filed late to the extent practicable. We may change this rulemaking in light of the comments we receive.

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.access.gpo.gov/su_docs/aces/aces140.html*; or

(3) Visiting the TSA's Law and Policy Web page at *http://www.tsa.dot.gov/public/index.jsp.*

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.

Summary of Proposed Rule

In conjunction with the establishment of a new system of records, Transportation Security Intelligence Service (TSIS) Operations Files (DHS/TSA 011), TSA proposes to exempt portions of the system from several provisions of the Privacy Act; the exemptions are claimed in accordance with the reasons explained below. The purpose of this system is to maintain 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. TSA also proposes to add 5 U.S.C. 552a(k)(1) as an authority to exempt the Personnel Background Investigation File System (DHS/TSA 004) from the provisions previously claimed for this system that allows TSA to maintain investigative and background records used to make suitability and eligibility determinations for employment. See 68 FR 49410, Aug. 18, 2003. The system is exempt from provisions of the Privacy Act in accordance with the reasons explained below. Finally, TSA proposes to add 5 U.S.C. 552a(j)(2) 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 subsection (e)(3) of the Privacy Act. See 68 FR 49410, Aug. 18, 2003. The systems are exempt from provisions of the Privacy Act in accordance with the reasons explained below. DHS/TSA 001 serves as an enforcement docket system while DHS/TSA 005 is maintained to facilitate the management of investigations into allegations or appearances of misconduct by current and former TSA employees or contractors and is being modified to cover investigations of security-related incidents and reviews of TSA programs and operations.

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. We have determined that there are no current or new information collection requirements associated with this proposed rule.

Analysis of Regulatory Impacts

This proposal is not a ''significant regulatory action'' within the meaning of Executive Order 12886. Because the economic impact should be minimal, further regulatory evaluation is not necessary. Moreover, I certify that this proposal 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

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 proposal 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

The energy impact of this document 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 Proposed Amendment

In consideration of the foregoing, the Transportation Security Administration proposes to amend part 1507 of chapter XII, title 49 of the Code of Federal Regulations, as follows:

PART 1507—PRIVACY ACT—EXEMPTIONS

1. The authority citation continues to read as follows:

Authority: 49 U.S.C. 114(1)(1), 5 U.S.C. 552a(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 security-sensitive information that 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 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).

(5) 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.

* * * * *

(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 for 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, while (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.

(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 information 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 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).

(5) 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 or 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.

* * * * *

(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 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 intelligence gathering operations 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 or apprehension, which undermines the entire system. Disclosure of the accounting may also reveal the existence of information that is classified or security-sensitive, 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 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 security-sensitive information that 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 December 3, 2004.

Lisa S. Dean,

Privacy Officer.

[FR Doc. 04–27097 Filed 12–9–04; 8:45 am]

BILLING CODE 4910–62–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

50 CFR Part 20

Service Regulations Committee Meeting

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of meeting.

SUMMARY: The Fish and Wildlife Service (hereinafter Service) will conduct an open meeting on January 27, 2005, to identify and discuss preliminary issues concerning the 2005–06 migratory bird hunting regulations.

DATES: The meeting will be held January 27, 2005.

ADDRESSES: The Service Regulations Committee will meet at the Arlington