construed to authorize any violation of such state laws that have greater restrictions.

Files will be destroyed only after the required period of maintenance, with a witness present, by either (1) a DHS or USCG Employee Assistance Program Administrator or an Employee Assistance Program Administrator from another organization that contracts with DHS or USCG for Employee Assistance Program services, or (2) by designated staff of a private or governmental organization under contract with DHS or USCG to provide document destruction services. The witness must be trained in the proper handling of records covered by the Privacy Act and 42 CFR Part 2.

Written records will be destroyed by shredding or burning. Records stored on hard drives will be destroyed using software tools which ensure the protection of the confidential information by making reconstruction or compromise by reuse impracticable. Records contained on back-up tapes/diskettes will be disposed by either physically destroying the tapes/diskettes or by deleting them using software tools which ensure the protection of the confidential information by making reconstruction or compromise by reuse impracticable.

Records located away from the destruction site shall be transferred to the destruction site in the confidential manner. The name and case coding number of the destroyed record will be maintained on a list of other destroyed records. No other information about Employee Assistance Program clients may be maintained once these files have been destroyed.

SYSTEM MANAGER AND ADDRESS:

Commandant, CG–1112, Office of Work-Life, United States Coast Guard Headquarters, 2100 2nd Street, SW., Washington, DC 20593–0001.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to Commandant, CG–1112, Office of Work-Life, United States Coast Guard Headquarters, 2100 2nd Street, SW., Washington, DC 20593–0001.

When seeking records about yourself from this system of records or any other USCG system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the USCG will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification Procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification Procedure'' above.

RECORD SOURCE CATEGORIES:

Information in this system is supplied from the following sources:

- USCG Employee Assistance Program: The client, the licensed mental health provider, and collateral sources and resources intended to help the client.
- USCG Workplace Violence and related Critical Incident Team: Investigation records, personnel records, critical incident team assembled to make recommendations to command, subject's supervisors, and the subject.
- USCG Critical Incident Stress Management-related records: Work-Life staff, Peers, Incident commander, command(s) affected, individuals impacted by incident, other support persons who may be mobilized to assist those impacted by the event.
- USCG Sexual Assault Prevention and Response Program: Victim, victim support person, medical personnel assisting victim, criminal investigations and investigators, and other support personnel intended to assist victim.
- USCG Victim Support Persons (VSP): The victim support person, Work-Life staff, VSP's or Victim Advocate's work supervisor, other support persons who may assist in training.
- USCG Critical Incident Stress Management Peer Volunteers: Peer, Peer's supervisor, Work-Life staff, and other support persons who may assist in training.
- Case records maintained by USCG Work-Life personnel on USCG Duty members who have demonstrated suicidal behavior: The patient, medical personnel, patient's command, and Work-Life staff and other support persons who may assist in helping the patient.
- Reports of USCG active duty suicidal behavior incidents, workplace violence incidents, critical incidents, and sexual assaults maintained by USCG Headquarters (CG–1112): Work-Life staff and others as described above under their related programs.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: October 22, 2008.

Hugo Teufel III

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–25967 Filed 10–30–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0106]

Privacy Act of 1974; U.S. Immigration and Customs Enforcement Trade Transparency Analysis and Research (TTAR) System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new system of records titled U.S. Immigration and Customs Enforcement (ICE) Trade Transparency Analysis and Research (TTAR). TTAR contains trade and financial data that is analyzed to generate leads for and otherwise support ICE investigations of trade-based money laundering, contraband smuggling, trade fraud and other financial crimes. The data in TTAR is generally maintained in the ICE Data Analysis and Research Trade Transparency System (DARTTS), a software application and data repository that conducts analysis of trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. Additionally, a Privacy Impact Assessment for DARTTS will be posted on the Department's privacy Web site.

(See *http://www.dhs.gov/privacy* and follow the link to ''Privacy Impact Assessments.'') Due to urgent homeland security and law enforcement mission needs, DARTTS is currently in operation. Recognizing that ICE is publishing a notice of system of records for an existing system, ICE will carefully consider public comments, apply appropriate revisions, and republish the TTAR notice of system of records within 180 days of receipt of comments. A proposed rulemaking is also published in this issue of the **Federal Register** in which the Department proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: The established system of records will be effective December 1, 2008. Written comments must be submitted on or before December 1, 2008. A revised TTAR notice of system of records that addresses public comments, responds to OMB direction, and includes other ICE changes will be published not later than May 29, 2009 and will supersede this notice of system of records.

ADDRESSES: You may submit comments, identified by DHS–2008–0106 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Docket:* For access to the docket to read background documents or comments received go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Lyn M. Rahilly (202–514–1900), Privacy Officer, U.S. Immigration and Customs Enforcement, 425 I Street, NW., Washington DC 20001, or Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Trade Transparency Analysis and Research (TTAR) system of records is owned by the ICE Office of Investigations Trade Transparency Unit (TTU) and is maintained for the purpose of enforcing criminal laws pertaining to trade through trade transparency. Trade transparency is the concept of examining U.S. and foreign trade data to identify anomalies in patterns of trade. Such anomalies can indicate trade-based money laundering or other import-export crimes that ICE is responsible for investigating, such as contraband smuggling, trafficking of counterfeit goods, misclassification of goods, and the over- or under-valuation of goods to hide the proceeds of illegal activities. TTAR contains trade and financial data received from U.S. Customs and Border Protection (CBP), U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN), other federal agencies and foreign governments. TTAR data is primarily related to international commercial trade and contains little information on the normal day-to-day activities of individual consumers.

As part of the trade transparency investigative process, ICE investigators and analysts must understand the relationships between importers and exporters and the financing for a set of trade transactions to determine which transactions are suspicious and warrant investigation. If performed manually, this process often involves hours of analysis of voluminous data for a particular case or operation. To automate and expedite this process, the former U.S. Customs Service created the Data Analysis and Research Trade Transparency System (DARTTS), a software application and data repository that conducts analysis of trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. DARTTS is specifically designed to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator. While DARTTS does increase the efficiency of data analysis, DARTTS does not allow ICE agents and analysts to obtain any data they could not otherwise access in the course of their investigative activities.

DARTTS does not seek to predict future behavior or ''profile'' individuals, i.e., look for individuals who meet a certain pattern of behavior that has been pre-determined to be suspect. Instead, it analyzes and identifies trade and financial transactions that are statistically anomalous. Investigators gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience to determine if the anomalous transactions are in fact suspicious and warrant further investigation. Not all anomalies lead to formal investigations. DARTTS can also identify links (relationships) between individuals or entities based on commonalities, such as identification numbers, addresses, or other information. These commonalities in and of themselves are not suspicious, but in the context of additional information they sometimes help investigators to identify potentially criminal activity and identify other suspicious transactions, witnesses, or suspects.

With the creation of the U.S. Department of Homeland Security (DHS) in 2003, the criminal investigative arm of the U.S. Customs Service, which included the TTU and the DARTTS system, was transferred to ICE. As part of DHS's ongoing effort to ensure legacy records transferred to DHS are maintained in compliance with the Privacy Act, ICE proposes to establish this new system of records to cover the data ICE maintains for trade transparency analysis, including the data maintained in DARTTS. A Privacy Impact Assessment (PIA) was conducted on DARTTS because it maintains personally identifiable information. The DARTTS PIA is available on the Department of Homeland Security (DHS) Privacy Office Web site at *http://www.dhs.gov/privacy.*

Individuals may request information about records pertaining to them stored in DARTTS as outlined in the ''Notification Procedure'' section below. ICE reserves the right to exempt various records from release pursuant to exemptions 5 U.S.C. 552a(j)(2) and (k)(2) of the Privacy Act.

Consistent with DHS's information sharing mission, information stored in the DARTTS may be shared with other DHS components, with foreign governments with whom DHS has entered into international information sharing agreements for trade data for the purpose of enforcing customs laws, and with appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States 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 for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the TTAR system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this new system of records to the Office of Management and Budget and to Congress.

SYSTEM OF RECORDS:

DHS/ICE–005.

SYSTEM NAME:

Trade Transparency Analysis and Research (TTAR).

SECURITY CLASSIFICATION:

Sensitive But Unclassified.

SYSTEM LOCATION:

Records are maintained at the Immigration and Customs Enforcement Headquarters in Washington, DC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: a) Individuals who, as importers, exporters, shippers, transporters, brokers, owners, purchasers, consignees, or agents thereof, participate in the import or export of goods to or from the U.S. or to or from nations with which the U.S. has entered an agreement to share trade information; and b) individuals who participate in financial transactions that are reported to the U.S. Treasury Department under the Bank Secrecy Act or other U.S. financial crimes laws and regulations (*e.g.*, individuals who participate in cash transactions exceeding $10,000; individuals who participate in a reportable suspicious financial transaction).

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Names;
- Addresses (home or business);
- Trade identifier numbers (*e.g.*, Importer ID, Exporter ID, Manufacturer ID);
- Social Security/tax identification numbers;
- Passport numbers;
- Account numbers (*e.g.*, bank account);
- Description and/or value of trade goods;
- Country of origin/export; and
- Description and/or value of financial transactions.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

18 U.S.C. 545 (Smuggling goods into the United States); 18 U.S.C. 1956 (Laundering of Monetary Instruments); and 19 U.S.C 1484 (Entry of Merchandise).

PURPOSE(S):

The purpose of this system is to enforce criminal laws pertaining to trade, financial crimes, smuggling, and fraud, specifically through the analysis of raw financial and trade data in order to identify potential violations of U.S. criminal laws pertaining to trade, financial crimes, smuggling, and fraud and to support existing criminal law enforcement investigations into related criminal activities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when (1) DHS or any component thereof; (2) any employee of DHS in his/her official capacity; (3) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or (4) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation; and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information, or harm to an individual; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or

implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

I. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

J. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

K. To a Federal, State, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

L. To a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

M. To international and foreign governmental authorities in accordance with law and formal or informal international agreements.

N. To Federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

O. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations where DHS is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by any of the personal identifiers stored in the system including name, business address, home address, importer ID, exporter ID, broker ID, manufacturer ID, social security number, trade and tax identifying numbers, passport number, or account number. Records may also be retrieved by non-personal information such as transaction date, entity/institution name, description of goods, value of transactions, and other information.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

RETENTION AND DISPOSAL:

ICE is in the process of drafting a proposed record retention schedule for the information maintained in DARTTS. ICE anticipates retaining the records in DARTTS for five years and then archiving records for five additional years, for a total retention period of ten years. The five-year retention period for records is necessary to create a data set large enough to effectively analyze anomalies and patterns of behavior in trade transactions. Records older than five years will be archived for five additional years and will only be used to provide a historical basis for anomalies in current trade activity. The original CD-ROMs containing the raw data will be retained for five years for the purpose of data integrity and system maintenance.

SYSTEM MANAGER AND ADDRESS:

Unit Chief, Trade Transparency Unit, ICE Office of Investigations, 425 I Street, NW., Washington DC 20536.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty or perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose form the Director, Disclosure and FOIA,

http://www.dhs.gov or 1–866–431–0486. In addition you should provide the following:

• An explanation of why you believe the Department would have information on you,

• Identify which component(s) of the Department you believe may have the information about you,

• Specify when you believe the records would have been created,

• Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,

• If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

(1) U.S. Customs and Border Protection (CBP) import data collecting using CBP Form 7501, ''Entry Summary.''

(2) U.S. Department of Commerce export data collected using Commerce Department Form 7525–V, ''Shipper's Export Declaration.''

(3) U.S. Exports of Merchandise Dataset (a publicly available aggregated U.S. export dataset purchased from the U.S. Department of Commerce).

(4) Foreign import and export data provided by partner countries pursuant to a Customs Mutual Assistance Agreement (CMAA) or other similar agreement.

(5) Financial Transaction Reports from Treasury Department's Financial Crimes Enforcement Network (FinCEN), specifically: (a) Currency Monetary Instrument Reports (CMIRs)—Declarations of currency or monetary instruments in excess of $10,000 made by persons coming into or leaving the United States; (b) Currency Transaction Reports (CTRs)—Deposits or withdrawals of $10,000 or more in currency into or from depository institutions; (c) Suspicious Activity Reports (SARs)—Information regarding suspicious financial transactions within depository institutions, casinos, and the securities and futures industry; and (d) Report of Cash Payments over $10,000 Received in a Trade or Business—Report of merchandise purchased with $10,000 or more in currency.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. 552a (k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

Dated: October 24, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–25968 Filed 10–30–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0018]

Privacy Act of 1974; Department of Homeland Security Employee Assistance Program Records System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security proposes to update and reissue one legacy record system: Justice/INS–019 INS Employment Assistance Program Treatment Referral Records. This system will allow the Department of Homeland Security to collect and maintain records on the Department's Employee Assistance Program. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice has been reviewed and updated to better reflect the Department's Employee Assistance Program record systems. This reclassified system, titled Employee Assistance Program Records, will be included in the Department's inventory of record systems.

DATES: Submit comments on or before *December 1, 2008.* This new system will be effective December 1, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0018 by one of the following methods:

• *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.

• *Fax:* 1–866–466–5370.

• *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

• *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov*, including any personal information provided.

• *Docket:* For access to the docket, to read background documents, or comments received go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107–296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records that concern the information relating to DHS's Employee Assistance Program (EAP).

As part of its efforts to streamline and consolidate its Privacy Act records systems, DHS is establishing a new agency-wide system of records under the Privacy Act (5 U.S.C. 552a) for DHS EAP records. The system will consist of records regarding individuals who have sought or been referred to counseling services provided through the EAP. These records may include identifying information, information about the presenting issue (e.g. relationships, behaviors, emotions, legal or financial issues, illegal drug use, alcohol abuse, or the experience of a traumatic event), and the actions taken by EAP.

In accordance with the Privacy Act of 1974 and as part of DHS's ongoing effort to review and update legacy system of record notices, DHS proposes to update and reissue one legacy record system: Justice/INS–019 INS Employment Assistance Program Treatment Referral Records (63 FR 3349 January 22, 1998). This system will allow DHS to collect and maintain records on DHS's