[Federal Register Volume 73, Number 245 (Friday, December 19, 2008)]
[Notices]
[Pages 77778-77782]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: E8-29807]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2008-0191]

Privacy Act of 1974; U.S. Customs and Border Protection--011 TECS System of Records Notice

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 is publishing a revised system of records notice for the system formerly known as the Treasury/CS.244, Treasury Enforcement Communication System, October 18, 2001, as a Department of Homeland Security system of records notice titled, DHS/CBP-011 TECS. Additionally, the Department is giving notice that it plans to consolidate into this newly revised system of records the following legacy system of records: Treasury/CS.272 Currency Declaration File, October 18, 2001; Treasury/CS.224 Suspect Persons Index, October 18, 2001; Justice/INS-032 National Automated Immigration Lookout System (NAILS), October 17, 2002; and Treasury/CS.262 Warnings to Importers in Lieu of Penalty, October 18, 2001. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been reviewed and updated to better reflect the Department of Homeland Security DHS/CBP-011 TECS, which is no longer an acronym.

TECS is an updated and modified version of the former Treasury

[[Page 77779]]

Enforcement Communications System, which is principally owned and managed by U.S. Customs and Border Protection and is its principal law enforcement and anti-terrorism data base system. TECS is established as an overarching law enforcement information collection, analysis, and sharing environment that securely links telecommunications devices and personal computers to a central system and database. This environment is comprised of several modules designed to collect, maintain, and screen data as well as conduct analysis, screening, and information sharing. TECS databases contain temporary and permanent enforcement, inspection and intelligence records relevant to the anti-terrorism and law enforcement mission of U.S. Customs and Border Protection and numerous other federal agencies that it supports. TECS also maintains limited information on those individuals who have been granted access to the system. Access is granted to those agencies which share a common need for data maintained in the system. TECS also allows direct access to other major law enforcement systems, including the Department of

Justice's National Crime Information Center (NCIC), the National Law Enforcement Telecommunications Systems (NLETS), and the Canadian Police Information Centre (CPIC).

In an effort to provide even more detailed information and transparency to the public, U.S. Customs and Border Protection has separately published System of Records Notices for the applicable subsets of data connected to TECS, including the DHS/CBP-006 Automated Targeting System (ATS) August 6, 2007, DHS/CBP-007 Border Crossing Information (BCI) July 25, 2008, DHS/CBP-005 Advanced Passenger Information System (APIS) last published November 18, 2008 and DHS/CBP-009 Non-Immigrant Information System (NIIS) being published concurrently with this SORN elsewhere in the Federal Register today.

Additionally, the Department is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the Federal Register. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been issued.

This system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before January 20, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS-2008-0191 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 please contact: Laurence E. Castelli (202-325-0280), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Regulations & Rulings, Mint Annex, 799 Ninth Street, NW., Washington, DC 20001-4501. For privacy issues contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. 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, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) have relied on preexisting Privacy Act system of records notices for the collection and maintenance of records that concern the Treasury Enforcement Communications System (TECS).

As part of its efforts to streamline and consolidate its record systems, DHS is updating and reissuing a DHS/CBP system of records under the Privacy Act (5 U.S.C. 552a) that deals with CBP's priority mission of preventing terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade.

On March 1, 2003, the United States Customs Service (owner of the Treasury Enforcement Communications System) was transferred from the

Department of the Treasury to the newly created Department of Homeland Security (``DHS'') and renamed ``Bureau of Customs and Border Protection.'' Subsequently, on April 23, 2007, a Notice was published in the Federal Register (72 FR 20131) to inform the public that the name of the Bureau of Customs and Border Protection had been changed by the Department of Homeland Security to ``U.S. Customs and Border Protection (CBP)''. Accordingly, inasmuch as the Treasury Enforcement Communications System is principally owned and managed by CBP and CBP is no longer part of the Department of the Treasury, the system formerly known as the Treasury Enforcement Communications System will now be known as DHS/CBP-011 TECS (no longer an acronym).

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 is publishing a revised system of records notice for the system formerly known as the Treasury/CS.244, Treasury Enforcement Communication System, (66 FR 52984 October 18, 2001), as a Department of Homeland Security system of records notice titled, DHS/CBP-011 TECS. Additionally, the Department is giving notice that it is retiring Treasury/CS.272 Currency Declaration File, (October 18, 2001 66 FR 52984) Treasury/CS.224 Suspect Persons Index (66 FR 52984 October 18, 2001) Justice/INS-032 National Automated Immigration Lookout System (NAILS) (67 FR 64136 October 17, 2002) and Treasury/CS.262 Warnings to Importers in lieu of Penalty (66 FR 52984 October 18, 2001), as they have been into this consolidated SORN. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been reviewed and updated to better reflect the Department of Homeland Security, U.S. Customs and Border Protection, and TECS.

DHS/CBP-011 TECS is an updated and modified version of the former Treasury Enforcement Communications System (TECS), which is principally owned and managed by U.S. Customs and Border Protection and is its principal law enforcement and anti-terrorism data base system. TECS is established as an overarching law enforcement information collection, analysis, and sharing environment that links telecommunications devices and personal computers securely to a central system and database. This environment is comprised of several modules designed to collect, maintain and screen data as well as conduct analysis, screening, and information sharing. TECS databases contain temporary and permanent enforcement, inspection, and intelligence records relevant to the anti-terrorism and law enforcement mission

[[Page 77780]]

of U.S. Customs and Border Protection and numerous other federal agencies that it supports. TECS also maintains limited information on those individuals who have been granted access to the system. Access is granted to those agencies which share a common need for data maintained in the system. TECS also allows direct access to other major law enforcement systems, including the Department of Justice's National Crime Information Center (NCIC), the National Law Enforcement Telecommunications Systems (NLETS) and the Canadian Police Information Centre (CPIC).

In an effort to provide even more detailed information and transparency to the public U.S. Customs and Border Protection has separately published System of Records Notices for the applicable subsets of data connected to TECS, including the DHS/CBP-006 Automated Targeting System (ATS) (August 6, 2007, 72 FR 43650), DHS/CBP-007 Border Crossing Information System (BCIS) (July 25, 2008, 73 FR 43457), DHS/CBP-005 Advanced Passenger Information System (APIS) (November 18, 2008, 73 FR 68435), and DHS/CBP-009 Non-Immigrant Information System (NIIS), which is being published concurrently with this SORN elsewhere

in the Federal Register today.

Additionally, the Department is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the Federal Register. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been published.

This system will be included in the Department of Homeland Security's inventory of record systems.

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 in individuals' records. 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. In the Privacy Act, an individual is defined to encompass United States citizens and lawful 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 to make agency recordkeeping practices transparent, to notify individuals regarding the uses of their records, and to assist the individual to more easily find such files within the agency. Below is a description of the TECS System of Records.

In accordance with 5 U.S.C. 552a(r), a report concerning this record system has been sent to the Office of Management and Budget and to the Congress.

System of Records: DHS/CBP-011

System name:

DHS/CBP-011 TECS.

Security classification:

Unclassified; Law Enforcement Sensitive.

System location:

This computer database is located at the U.S. Customs and Border Protection National Data Center in the Washington DC area. TECS will be migrated to other DHS Datacenters. Computer terminals are located at CBP sites and ports throughout the United States and at CBP Headquarters, Washington, DC, as well as appropriate facilities under the jurisdiction of the U.S. Department of Homeland Security (DHS) and other locations at which officers of DHS may be posted or operate to facilitate DHS's mission of homeland security. Terminals may also be located at appropriate facilities for other participating government agencies pursuant to agreement.

Categories of individuals covered by the system:

Violators or suspected violators of laws enforced or administered by DHS (some of whom have been apprehended by officers of DHS);

Individuals who are suspected of, or who have been

arrested for, thefts from international commerce;
Convicted violators of laws enforced or administered by DHS and/or drug laws in the United States and foreign countries;
Persons with outstanding warrants--Federal or state;
Victims of any violation of the laws enforced or administered by DHS;
Owners, operators and/or passengers of vehicles, vessels or aircraft traveling across U.S. borders or through other locations where CBP maintains an enforcement or operational presence;
Persons traveling across U.S. borders or through other locations where CBP maintains an enforcement or operational presence and who are determined to be related to a law enforcement context;
Persons identified by Center for Disease Control (CDC), U.S. Health and Human Services as ``No Boards'' because of a highly contagious communicable disease through the Advance Passenger Information System in connection with trying to board an aircraft to travel internationally;
Individuals who have been issued a CBP detention or warning;
Individuals who may pose a threat to the United States; and
Individuals who have been given access to TECS for authorized purposes.

Categories of records covered by the system:
Various types of information from a variety of Federal, state, local, and foreign sources, which contribute to effective law enforcement and counterterrorism efforts, may be maintained in this system of records. Records include, but are not limited to, records pertaining to known or suspected violators, wanted persons, persons of interest for law enforcement and counterterrorism purposes, reference information, regulatory and compliance data. Information about individuals includes, but is not limited to full name, alias, date of birth, address, physical description, various identification numbers (e.g., social security number, alien number, I-94 number, seizure number), details and circumstances of a search, arrest, or seizure, case information such as merchandise and values, methods of theft.

Authority for maintenance of the system:
Section 5 U.S.C. 301; Homeland Security Act of 2002, Pub. L. 107-296; the Tariff Act of 1930, as amended; Title 18, United States Code, Chapter 27; the Immigration and Nationality Act.

Purpose
The purpose of this system is to track individuals who have violated or are suspected of violating a law or regulation that is enforced or administered by CBP, to provide a record of any inspections conducted at

[[Page 77781]]

the border by CBP, to determine admissibility into the United States, and to record information regarding individuals, firms, and organizations to whom DHS/CBP has issued detentions and warnings. Additionally, this system of records covers individuals who have been given access to TECS for authorized purposes.

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 it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee of DHS or any component in his/her official capacity;

3. Any employee of DHS or any component in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. The U.S. or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS or CBP 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 or CBP collected the records.

B. To a congressional office 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 or CBP suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS or CBP 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, CBP, or another agency or entity) or harm to the individual who relies upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS or CBP'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 or CBP, 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/CBP officers and employees.

G. 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.

H. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil or criminal discovery, litigation, or settlement negotiations, or in response to a subpoena from a court of competent jurisdiction.

I. 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.

J. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

K. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

L. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or for combating other significant public health threats.

M. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate in the proper performance of the official duties of the person making the disclosure;

N. To the news media and the public, with the approval of the DHS Chief Privacy Officer in consultation with counsel, as appropriate, 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 CBP or is necessary to demonstrate the accountability of CBP'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.

O. 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.

Disclosure to consumer reporting agencies:

None.

[[Page 77782]]

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

The data is stored electronically at the National Data Center and other DHS Data Centers for current data and offsite at an alternative data storage facility for historical logs and system backups.

Retrievability:

The data is retrievable by name, address, unique identifiers or in association with an enforcement report or other system document.

Safeguards:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: restricting access to those with a ``need to know''; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

TECS also monitors source systems for changes to the source data. The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. TECS information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive information security program.

Access to TECS is controlled through a security subsystem, which is used to grant access to TECS information on a ``need-to-know'' basis.

Retention and Disposal:

The majority of information collected in TECS is used for law enforcement and counterterrorism purposes. Records in the system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration.

The retention period for information maintained in TECS is seventy-five (75) years from the date of the collection of the information or for the life of the law enforcement matter to support that activity and other enforcement activities that may become related. TECS collects information directly from authorized users.

System Manager and address:

Assistant Commissioner, Office of Information Technology, Passenger Systems Program Office, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, CBP will consider individual requests to determine whether or not information may be released. Thus, 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 CBP's FOIA Officer, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

When seeking records about yourself from this system of records or any other CBP 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 CBP may 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:

This system contains investigatory material compiled for law enforcement and counterterrorism purposes whose sources need not be reported.

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)(4)(I), (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), (e)(4)(I), and (f). In addition, to the extent a record contains information from other exempt systems of records, CBP will rely on the exemptions claimed for those systems.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29807 Filed 12-18-08; 8:45 am]

BILLING CODE 4410-10-P