[Federal Register: December 19, 2008 (Volume 73, Number 245)]
[Notices]
[Page 77759-77764]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr19de08-128]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2008-0150]

Privacy Act of 1974; U.S. Customs and Border Protection--015 Automated Commercial System, 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 the following legacy record system, Treasury/CS.278 Automated

[[Page 77760]]

Commercial System (October 18, 2001) as a Department of Homeland Security system of records notice titled, U.S. Customs and Border Protection Automated Commercial System. The Customs and Border Protection Automated Commercial System is a comprehensive system used by Department of Homeland Security, U.S. Customs and Border Protection to track, control, and process all commercial goods imported into the United States. This legacy system will now also collect additional data via its Automated Broker Interface and Vessel Automated Manifest System. 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 U.S. Customs and Border Protection--015 Automated Commercial System record system. This reissued system will be included in the Department of Homeland Security's inventory of record systems.

DATES: The established system of records will be effective January 20, 2009. Written comments must be submitted on or before January 20, 2009.

ADDRESSES: You may submit comments, identified by DHS-2008-0150 by one of the following methods:

Federal e-Rulemaking Portal: http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=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://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&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://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&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 please 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

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. The Automated Commercial System (ACS) is the comprehensive system used by U.S. Customs and Border Protection to track, control, and process all commercial goods imported into the United States. ACS is a sophisticated and integrated large-scale business-oriented system which employs multiple modules to perform discrete aspects of its functionality, including receiving data transmissions from a variety of parties involved in international commercial transactions and providing CBP with the capability to track both the transport transactions and the financial transactions associated with the movement of merchandise through international commerce. Through the use of Electronic Data Interchange (EDI), ACS facilitates merchandise processing, significantly cuts costs, and reduces paperwork requirements for both Customs and the importing community.

ACS also provides the following:

A. Cargo Selectivity

CBP uses the ACS Cargo Selectivity System to sort high risk cargo from low risk cargo and to determine the type of examination required. Cargo selectivity accepts data transmitted through ABI and compares it against established criteria. CBP uses the Cargo Selectivity System, a module of ACS, to process manifests and National In-bond entries in order to identify the CBP inspection and examination status of specific bills of lading for imported merchandise. Cargo Selectivity facilitates more efficient and effective cargo processing by ensuring cargo that requires additional screening receives it and that which is lower risk does not.

B. Entry Summary Selectivity

The Entry Summary Selectivity system of ACS screens the review of entry summary data. Using line item data transmitted through ABI, the system matches national and local selectivity criteria against entry summary data to assess risk by importer, tariff number, country of origin, manufacturer, and value. The system captures paperless summary activity, discrepant summary findings, and line item team assignment data.

C. Border Cargo

The Border Cargo Selectivity system of ACS determines risk assessment and examination requirements for high volume borders (i.e., ports of entry). The system uses the same screening process as the Cargo Selectivity system. The Border Cargo Selectivity system will soon be enhanced to allow ABI filers to transmit manifest information.

D. Quota

The ACS Quota system tracks quantity controls on imported merchandise. It also tracks visas from other countries. (Visas determine the amount of exports allowed for certain countries.) The Quota system checks the quantities against the visas and transmits this information to the country of origin. The ACS quota and visa controls simplify reconciliation of imports and exports.

E. Paperless Entry

Paperless entry processing eliminates the need for ABI participants to file a Customs Form 3461, Entry/Immediate Delivery, if certain criteria are met and the merchandise does not require examination. Carriers who participate in AMS will receive electronic notifications when merchandise is available for release.

F. Automated Invoice Interface (AII)

AII allows filers to send electronic invoice information to Customs. This information is transmitted to Customs using either ABI record formats or the EDIFACT CUSDEC (Customs declaration). When EDIFACT is used, the filer also transmits data that is normally on the CF-3461 for cargo release, as well as the entry summary CF-7501, invoice data, and other government agency data.

G. Drawback

Filers can submit a drawback claim to Customs on a diskette or through ABI. This ensures that the data is quickly and accurately recorded in ACS and results in faster claim processing and issuance of the drawback payment. Immediate acceptance or rejection of data is available.

H. Protest

The ABI electronic protest system allows ABI participants to file, amend, and query the following types of actions:

Protests against decisions of the Customs Service under 19 U.S. C. 1514.

Petitions for refunds of Customs duties or corrections of errors requiring reliquidation pursuant to 19 U.S.C. 1520(c) and (d).

Interventions in an importer's protest by an exporter or producer of merchandise from a country that is a party to the North American Free Trade

Agreement under Section 181.115 of the Customs Regulations.

Once filed, protests can be amended and additional arguments submitted to:

Apply for further review (when not requested at time of filing).

Assert additional claims or challenge an additional decision.

Submit alternative claims and additional grounds or arguments.

Request review of denial of further review.

Request denial of the protest be voided.

The protest, petition, or intervention can be transmitted remotely from any location. Customs views and processes the protest on-line. An automatic notification routine keeps the filer informed of any change in status, including final disposition.

I. Remote Location Filing

Remote Location Filing (RLF) is a pilot program which allows an approved participant to electronically file a formal or informal entry of merchandise with Customs from a location within the United States other than the port of arrival (POA) or the designated examination site (DES). Such merchandise, upon clearance by CBP, may enter the commerce of the United States.

J. National In-bond

The National In-bond system tracks cargo en route in the United States. Using departure, arrival, and closure data, the In-bond system tracks cargo from the point of unlading to the port of entry or exportation. The In-bond system is incorporated within AMS. AMS retains control over all sea in-bond movements (both conventional and paperless) that are associated with automated bills of lading.

K. Paperless Master In-bond

The Paperless Master In-bond program controls the movement and disposition of master in-bond (MIB) shipments from the carrier's custody at the port of unlading to the same carrier's custody at the port of destination. This program utilizes the data already available in AMS, eliminating the need for paper documentation.

To help prevent terrorist weapons from being transported to the United States, vessel carriers bringing cargo to the United States are required to transmit certain information to Customs and Border Protection (CBP) about the cargo they are transporting prior to lading that cargo at foreign ports of entry. CBP is issuing an interim final rule that requires both importers and carriers to submit additional information pertaining to cargo to CBP before the cargo is brought into the United States by vessel. This information must be submitted to CBP

by way of a CBP-approved electronic data interchange system. The required information is necessary to improve CBP's ability to identify high-risk shipments so as to prevent smuggling and ensure cargo safety and security, as required by section 203 of the Security and Accountability for Every (SAFE) Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002.

The proposed rule was known to the trade as both the ``Importer Security Filing proposal'' and the ``10 + 2 proposal.'' The name ``10 + 2'' is shorthand for the number of advance data elements CBP was proposing to collect. Carriers would be generally required to submit two additional data elements--a vessel stow plan and container status messages regarding certain events relating to containers loaded on vessels destined to the United States--to the elements they are already required to electronically transmit in advance (the ``2'' of ``10+2''); and importers, as defined in the proposed regulations, would be required to submit ten data elements--an Importer Security Filing containing ten data elements (the ``10'' of ``10+2'').

ACS has two principal methods for electronic data interchange: The Automated Broker Interface (ABI) and the Automated Manifest System (AMS). Under the ``10+2'' program, importers, who submit the Importer Security Filing (ISF), will use either ABI or Vessel AMS to provide their information to CBP. ACS, upon receipt of the ISF, will transfer the data to the Automated Targeting System (ATS) for screening and targeting purposes. Once screened the ISF data will be returned with embedded targeting links to ACS to be maintained in accordance with the ACS stated retention policy.

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 maintenance of records that concern the tracking, controlling, and processing of all commercial goods imported into the United States.

This collection satisfies the requirements of Section 203 of the Security and Accountability for Every Port Act of 2006 (Pub. L. 109-347, 120 Stat. 1884 (SAFE Port Act)).

Consistent with DHS's information sharing mission, information stored in the Automated Commercial System may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS/CBP 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.

To provide notice and transparency to the public, the Department of Homeland Security, U.S. Customs and Border Protection announces an amendment to an existing legacy Privacy Act system of records, the Automated Commercial System, a comprehensive system used by U.S. Customs and Border Protection to track, control, and process all commercial goods imported into the United States. This legacy system will now also collect additional data via the Automated Broker Interface and Vessel Automated Manifest System.

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 the following legacy record system,

Treasury/CS.278 Automated Commercial System (66 FR 52984 October 18, 2001), as a DHS/CBP system of records notice titled, U.S. Customs and Border Protection Automated Commercial System. Categories of individuals and categories of records have been reviewed, and the routine uses of this legacy system of records notice have been updated to better reflect the DHS/CBP Automated Commercial System record system. This reissued system will be included in DHS'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. 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 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 in order to make agency recordkeeping 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 Automated Commercial System system of records.

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

System of Records
DHS/CBP--015

System name:
U.S. Customs and Border Protection--015 Automated Commercial System

Security classification:
Unclassified.

System location:
Records are maintained at the CBP Headquarters in Washington, DC and field offices.

Categories of individuals covered by the system:
Categories of individuals covered by this system include: CBP employees and individuals involved in the import trade.

Categories of records in the system:
Categories of records in this system include:
Individual's name;
Social Security Number (SSN), if collected;
Address;
CBP employee names;
CBP employee SSN;
Importer of record number, which can be the IRS Employer Identification Number (EIN), SSN, or a Customs-assigned number;
Importer name and address;
Type of importation bond;
Importation bond expiration date;
Surety code;
Violation statistics;
Protest information;
Customhouse broker number;
Customhouse name;
Customhouse address;
Bond agent name;
Bond agent SSN;
Surety code (non-SSN);
Surety name;
Customs bond information;
Liquidator identification (non-SSN);
Foreign Manufacturer/Shipper identification code;
Foreign Manufacturer/Shipper name;
Foreign Manufacturer/Shipper address;
Carrier names;
Carrier codes (non SSN) (Standard Carrier Agent Code (SCA) for vessel carriers, International Air Transport Association (IATA) for air carriers);
Manufacturer (or supplier) name;
Seller name;
Buyer name;
Ship to party name;
Container stuffing location;
Consolidator (stuffer);
Foreign trade zone applicant identification number;
Consignee number(s);
Country of origin;
Commodity HTSUS number;
Booking party;
Foreign port of unlading;
Place of delivery; and
Ship to party.

Authority for maintenance of the system:
19 U.S.C. 66, 1431, 1448, 1481, 1484, 1505, 1514 and 1624, section 203 of the Security and Accountability for Every (SAFE) Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002.

Purpose(s):
The purpose of this system is to track, control, and process all commercial goods imported into the United States, and to improve CBP's ability to identify high-risk shipments so as to prevent smuggling and

ensure cargo safety and security. As part of CBP identifying high risk shipments for border security and counterterrorism purposes, the system includes information relating to individuals and their relationship to the merchandise as documented in the Importer Security Filing (ISF).

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/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/CBP 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; 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 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.

H. 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.

I. To the Bureau of the Census to provide information on foreign trade data.

J. To a Federal agency, pursuant to the International Trade Data System Memorandum of Understanding, consistent with the receiving agency's legal authority to collect information pertaining to and/or regulate transactions in international trade.

K. 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.

L. To a Federal, State, local, tribal, territorial, foreign, or international agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

M. 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 discovery, litigation, or settlement negotiations, in response to a subpoena, or in connection with criminal law proceedings;

N. To third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

O. To the Department of Justice, the United States Attorney's Office, or a consumer reporting agency for further collection action on any delinquent debt when circumstances warrant;

P. 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;

Q. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of

responsibility;

R. 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 of life or property; and

S. To a consumer reporting agency related to owing the U.S. Government money in accordance with 15 U.S.C 1681 et seq.

Disclosure to consumer reporting agencies:

Yes, in accordance with the provision of 15 U.S.C. 1681 et seq.

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 that are stored electronically are stored on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

Records may be retrieved by identification codes and/or name.

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:

The Importer Security Filing is retained for fifteen years from date of submission unless it becomes linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; individuals, and routes of concern; or other defined sets of circumstances) for which it will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related. All other records are maintained for a period of six years from the date of entry.

System Manager and address:

Director, Office of Automated Systems, CBP Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 is responsible for all data maintained in the files.

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 CBP's FOIA Officer, 1300 Pennsylvania Avenue, NW., Washington, DC 20229. 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

[[Page 77764]]

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 from the Director, Disclosure and FOIA, http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=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:

Records are obtained by authorized Customs forms or electronic formats from individuals and/or companies incidental to the conduct of foreign trade and required by CBP in administering the tariff laws and regulations of the United States.

Exemptions claimed for the system:

Information in the system may be shared with law enforcement and/or intelligence agencies pursuant to the above routine uses. The Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agencies has sought particular records may affect ongoing law enforcement or intelligence activity. As such pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), DHS will claim exemption from (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.