9111-28

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0017]

Privacy Act of 1974; Department of Homeland Security U.S. Immigration and Customs Enforcement – 005 Trade Transparency Analysis and Research (TTAR) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of amendment of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to amend a current Department of Homeland Security system of records titled, "Department of Homeland Security/Immigration and Customs Enforcement-005 Trade Transparency Analysis and Research (TTAR) System of Records." This system of records is being modified to include new categories of individuals, categories of records, and purposes. The system is also being updated to update, consolidate, and clarify the existing routine uses, to reflect a proposed change to the retention period of the system's data, and to update and simplify the description of the record sources. The data in the TTAR system of records is generally maintained in the ICE Data Analysis and Research Trade Transparency System (DARTTS), which is 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, an update to the Privacy Impact Assessment for DARTTS has been posted on the Department's privacy web site (see

www.dhs.gov/privacy). The exemptions for the existing system of records notice will continue to be applicable for this system of records notice. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0017 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 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 Rahilly, Privacy Officer, (202-732-3300), U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536, e-mail: ICEPrivacy@dhs.gov, or Jonathan R. Cantor, Acting Chief Privacy Officer, (202-343-1717), Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) proposes to amend a current DHS system of records titled "DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) System of Records." This system of records is being modified to include new categories of individuals, categories of records, and purposes. The system is also being updated to update, consolidate, and clarify the existing routine uses, to reflect a proposed change to the retention period of the data, and to update and simplify the description of the record sources.

With the previously-published DARTTS PIA update, ICE is also notifying the public of three other changes to the TTAR SORN's associated IT system, DARTTS. First, ICE is expanding the use of DARTTS within DHS to permit select U.S. Customs and Border Protection (CBP) customs officers and import specialists to access and use the system to conduct trade transparency analysis. These CBP employees use DARTTS in support of the CBP mission to enforce U.S. trade laws and ensure the collection of all lawfully owed revenue from trade activities.

Second, ICE is establishing a separate instance of DARTTS for use by foreign government partners that operate trade transparency units and have customs information sharing agreements with the United States. This new "Foreign DARTTS" system is maintained in a secure, web-based environment hosted by ICE. Foreign DARTTS permits authorized foreign partners to use the DARTTS tools to analyze a more limited set of DARTTS data in support of their own trade-based investigations. Third, DARTTS

will be modified in the near future to permit authorized ICE and CBP personnel to access DARTTS via mobile devices. The DARTTS PIA update is available at www.dhs.gov/privacy.

The TTAR system of records and its associated IT system, DARTTS, are owned by ICE Homeland Security Investigations (HSI) and maintained for the purpose of enforcing criminal and civil 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 HSI 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.

As part of the trade transparency investigative process, DHS law enforcement personnel 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. The TTAR system of records supports the operation of DARTTS, which is 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, it does not allow DHS law enforcement personnel to obtain any data they could not otherwise access in the course of their law enforcement activities.

Consistent with DHS's information sharing mission, information stored in the DHS/ICE-005 TTAR System of Records may be shared with other DHS components. In accordance with the routine uses set forth in this system of records notice, this information may also be disclosed externally to federal, state, local, tribal, territorial, 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 aforementioned routine uses.

II. Changes to the System of Records

In this amendment, DHS is expanding the categories of individuals covered by this system of records to include two new categories: Specially Designated Nationals (SDN) as defined by 31 C.F.R. § 500.306, and individuals identified in TECS subject records created by ICE and CBP. The SDN List is an economic and trade sanctions program based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, and other threats to the national security, foreign policy or economy of the United States. Including the SDN List in DARTTS allows HSI users to quickly identify international trade and/or financial transactions that are associated with a specially designated individual or entity, which allows HSI to take appropriate investigative actions in a timely and more efficient manner.

TECS subject records includes violators or suspected violators of laws enforced or administered by ICE and CBP; witnesses associated with ICE and CBP enforcement actions; persons who own or operate businesses, property, vehicles or other property that

is in a TECS subject record; and individuals applying for a license issued by DHS or for which DHS conducts a background investigation in support of the licensing agency. Including ICE and CBP subject records in DARTTS allows users to quickly determine when an entity being researched in DARTTS is already part of a pending HSI investigation or was involved in an investigation that is now closed.

In this amendment, DHS is also including three new categories of records that are covered by this system of records: (1) TECS subject records related to an ICE or CBP law enforcement matter; (2) Customs or Homeland Security licensing information, related to applications by individuals or businesses to hold a specific license issued by DHS or for which DHS conducts a background investigation in support of the licensing agency; and (3) Information obtained from the SDN List maintained by the U.S. Department of the Treasury. DHS is also restructuring the categories of records into related groups instead of simply listing the data elements.

In this amendment, DHS is modifying and clarifying the system location to make clear that this system of records describes data maintained in DARTTS. DHS is also modifying the authority citations to include additional authorities that support the ICE and CBP mission for which trade transparency analysis is performed. DHS has also added citations to authorities that protect some of the information in DARTTS, such as the Trade Secrets Act and the Bank Secrecy Act.

In this amendment, DHS is also broadening the purpose section to include the civil enforcement aspects of CBP's mission that the system will now support. DHS is also adding two additional purposes associated with the launch of Foreign DARTTS to describe the reasons the system will be used by foreign government partners. Finally,

DHS has added a new purpose that describes the law enforcement, homeland security, and public safety purposes that all ICE law enforcement systems are generally maintained to support.

In this amendment, DHS is proposing to reword several routine uses to improve their clarity and to reduce redundancy. DHS is also deleting one routine use as it was found to be redundant to other existing routine uses. Finally, DHS is proposing to add the following four routine uses: (1) to permit sharing with courts, magistrates, counsel, parties and witnesses when relevant and necessary to litigation to which DHS is a party or in which it has an interest (Routine Use N); (2) to permit sharing with prospective parties and their counsel in advance of the initiation of formal litigation proceedings for settlement negotiation purposes (Routine Use O); (3) to permit sharing with other domestic or foreign agencies or entities for information or assistance in processing a claim for redress in connection with the operations of a DHS component or program (Routine Use P); and (4) to permit sharing with former employees of DHS when DHS requires information or consultation assistance from them regarding a matter within that person's former area of responsibility (Routine Use Q). The new proposed routine uses are intended to permit information sharing in the event that information covered by this system of records becomes relevant to an actual or potential claim in litigation or other proceedings, to a pending request from an individual for redress from DHS, or in the event that a matter arises in which DHS must share information with a former employee to obtain information or consultation assistance from that individual.

In this amendment, DHS is also notifying the public of its intention to modify the retention period of information maintained in this system of records. Currently,

DARTTS data is maintained in production for five years, archived for an additional five years, and then deleted. DHS proposes to maintain the data in production for ten years and then delete the data. The retention period is also proposed to change from five to ten years for the original CD-ROMs, external storage devices, or electronic data transfers containing raw data that is input into DARTTS.

Finally, in this amendment, DHS is simplifying and updating the description of the record sources for this system of records. The U.S. Department of the Treasury is being added because it is the source for the SDN List.

The exemptions for the existing system of records notice will continue to be applicable for this system of records notice. This updated system will be included in the Department of Homeland Security's inventory of record systems.

III. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses, and disseminates 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 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 U.S. 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.

Below is the description of the amended DHS/ICE-005 Trade Transparency

Analysis and Research System of Records.

In accordance with 5 U.S.C. § 552a(r), DHS has provided a report of this 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) System

Security classification:

Sensitive But Unclassified

System location:

Records are maintained in the Data Analysis and Research for Trade Transparency System (DARTTS), which is an IT system owned and operated by U.S. Immigration and Customs Enforcement (ICE) and maintained in a Department of Homeland Security (DHS) data center. The DARTTS application is maintained on the ICE Network and also at ICE Attaché Offices abroad.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

(1) 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 United States or to or from nations with which the United States has entered an agreement to share trade information;

(2) 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);

(3) Specially Designated Nationals as defined by 31 C.F.R. § 500.306; and

(4) Individuals identified in TECS subject records created by ICE and U.S. Customs and Border Protection (CBP), including violators or suspected violators of laws enforced or administered by ICE and CBP; witnesses associated with ICE and CBP enforcement actions; persons who own or operate businesses, property, vehicles or other property that is in a TECS subject record; and individuals applying for a license issued by DHS or for which DHS conducts a background investigation in support of the licensing agency.

Categories of records in the system:

Categories of records in this system include:

(1) Biographic and other identifying information about individuals, including names; dates of birth; Social Security/tax identification numbers; passport information (number and country of issuance); citizenship; location and contact information (such as home, business, and email addresses and telephone numbers); and other identification numbers (e.g., Alien Registration Number, driver's license number, etc.).

(2) Customs, trade, and financial data associated with an individual, including trade identifier numbers (e.g., Importer ID, Exporter ID, Manufacturer ID); account numbers (e.g., bank account, electronic fund transfer number); description and/or value of trade goods; country of origin/export; description and/or value of financial transactions; vehicle, vessel and/or aircraft information; and other business information.

(3) TECS subject records related to an ICE or CBP law enforcement matter.

(4) Customs or Homeland Security licensing information, related to applications by individuals or businesses to hold or retain a Customs broker's license, or operate a Customs-bonded warehouse, or be a bonded carrier or bonded cartman.

(5) Information obtained from the Specially Designated Nationals List maintained by the U.S. Department of the Treasury, including individual's name, aliases, address, date of birth, place of birth, citizenship, nationality, passport information, and program under which designation was made.

Authority for maintenance of the system:

The Tariff Act of 1930, as amended, 19 U.S.C. Chapter 4; 18 U.S.C. § 545 (Smuggling goods into the United States); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); 19 U.S.C § 1484 (Entry of Merchandise); 18 U.S.C. § 544 (Smuggling goods out of the United States); 18 U.S.C. § 371 (Conspiracy); and 50 U.S.C. §§ 1701-1706 (International Emergency Economic Powers Act); 19 U.S.C. § 2071 note (Cargo Information). Certain information in this system of records is also regulated under 18 U.S.C. § 1905 (Trade Secrets Act) and 31 U.S.C. § 5311-5330 (Bank Secrecy Act).

Purpose(s):

The purpose of this system is to support:

(1) The enforcement of criminal and civil laws pertaining to trade, financial crimes, smuggling, and fraud, and the collection of all lawfully owned revenue from trade activities, specifically through the analysis of raw financial and trade data in order to identify potential violations of U.S. criminal and civil laws pertaining to trade, financial activities, smuggling, and fraud;

(2) Existing criminal law enforcement investigations into related criminal

activities and civil enforcement actions to recover revenue and assess fines and penalties;

(3) The sharing of raw trade data and analytical capabilities with foreign government partners to further those governments' abilities to identify, disrupt, and prosecute criminal and civil violations of laws pertaining to trade, financial activities, smuggling, and fraud;

(4) The cooperation and collaboration between the United States and foreign government partners on investigations into transnational activities that violate criminal and civil laws pertaining to trade, financial activities, smuggling, and fraud; and

(5) The identification of potential criminal activity, immigration violations, and threats to homeland security: to uphold and enforce the law; and to ensure public safety.

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 (DOJ) (including United States Attorneys' Offices) 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 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.

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 (NARA) 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 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) DHS has determined that as a result of the suspected or confirmed compromise there is a risk of: identity theft or fraud, harm to the economic or property interests, harm to an individual, 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, interns, trainees, students, 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 federal, state, local, tribal, territorial, or foreign government agencies, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates or to elicit information required by DHS to carry out its functions and statutory mandates.

H. To federal, state, local, tribal, territorial, or foreign government 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, criminal, or regulatory laws.

I. To federal, state, local, tribal, or territorial government agencies, or other entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information

for the purposes of national security, intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

J. To federal, state, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

K. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

L. To federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or where such disclosure is to support the conduct of national intelligence and security investigations or assist in antiterrorism efforts.

M. To federal, state, local, tribal, territorial, international, or foreign government agencies or multinational governmental organizations where DHS desires to exchange relevant data for the purpose of developing, testing, or implementing new software or technology whose purpose is related to the purpose of this system of records.

N. To courts, magistrates, administrative tribunals, opposing counsel, parties, and witnesses, in the course of immigration, civil, or criminal proceedings (including discovery, presentation of evidence, and settlement negotiations) before a court or

adjudicative body when any of the following is a party to or have an interest in the litigation:

(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 the government has agreed to represent the employee; or

(4) the United States, where DHS determines that litigation is likely to affect DHS or any of its components;

and when DHS determines that use of such records is relevant and necessary to the litigation and is compatible with the purposes for which the records were collected.

O. To prospective claimants and their attorneys for the purpose of negotiating the settlement of an actual or prospective claim against DHS or its current or former employees, in advance of the initiation of formal litigation or proceedings.

P. To federal, state, local, tribal, territorial, international, or foreign government agencies or entities for the purpose of consulting with those agencies or entities:

(1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program;

(2) to verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or

to verify the accuracy of information submitted by an individual who has requested redress on behalf of another individual.

Q. To a former employee of DHS for the purpose of responding to an official inquiry by federal, state, local, tribal, or territorial government agencies or professional

licensing authorities; or facilitating communications with a former employee that may be necessary for personnel-related matters or other official purposes where DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

R. 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.

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.

Retention and disposal:

ICE is in the process of modifying the records schedule for the information maintained in this system of records. Currently the data is maintained in the DARTTS system for five years, archived for an additional five years and then deleted. ICE is now proposing to maintain the data in DARTTS for ten years and then delete the data. The original CD-ROMs, external storage devices or electronic data transfers containing raw data that is uploaded into DARTTS would also be retained for ten years to ensure data integrity and for system maintenance purposes.

System Manager and address:

Unit Chief, Trade Transparency Unit, ICE Homeland Security Investigations, 500 12th Street, SW, Mail Stop 5103, Washington, D.C. 20536.

Notification procedure:

The Secretary of Homeland Security has exempted this system from notification, access, and amendment because of the law enforcement nature of the information. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records. To the extent that a record is exempted in a source system, the exemption will continue to apply. However, ICE will review requests on a case by case to determine if release of the information is appropriate. After conferring with the appropriate component or agency, as applicable, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Additionally, ICE and DHS are not exempting any records that were ingested or indexed by TTAR where the source system of records already provides access and/or amendment under the Privacy Act. 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 ICE Freedom of Information Act 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 and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 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 of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, 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; and
- 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) 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:

Records are obtained from U.S. Customs and Border Protection (CBP), U.S. Department of Commerce, U.S. Department of the Treasury, and foreign countries pursuant to international agreements or arrangements.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted portions of this system. Pursuant to 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: August 16. 2012

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-21691 Filed 08/31/2012 at 8:45 am; Publication Date: 09/04/2012]