DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0074]

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: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue 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 (1) update existing and include new categories of individuals, (2) clarify existing and include new categories of records, (3) reflect a proposed change to the retention period of the system's data, and (4) update the description of the record sources. In addition, the Department is notifying the public of changes triggered by the replacement of the TTAR SORN's associated IT system, the Data Analysis and Research for Trade Transparency System (DARTTS), with FALCON-DARTTS, which replicates the functionality of and serves the same user groups as legacy DARTTS. The TTAR SORN is also being updated to expand coverage to a new IT system called FALCON-Roadrunner. The FALCON-DARTTS and FALCON-Roadrunner Privacy Impact Assessments are posted on the Department privacy website (*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-2014-0074 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: Karen L. Neuman, 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: For general questions, please contact: Lyn Rahilly, Privacy Officer, U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536, phone: 202-732-3300, e-mail: ICEPrivacy@dhs.gov. For privacy questions, please contact: Karen Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528, phone: 202-343-1717.

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 update and reissue a current DHS system of records titled "DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) System of Records." This system allows ICE Homeland Security Investigations (HSI) to collect and maintain records for the purpose of enforcing criminal and civil laws pertaining to customs violations, including trade-based money laundering. With this update, ICE is notifying the public of changes triggered by the replacement of the TTAR SORN's associated IT system, the Data Analysis and Research for Trade Transparency System (DARTTS), with FALCON-DARTTS, which replicates the functionality of and serves the same user groups as legacy DARTTS. The TTAR SORN is also being updated to expand coverage to a new ICE IT system, FALCON-Roadrunner.

The FALCON Environment

In 2012, HSI created a new IT environment called "FALCON" to support its law enforcement and criminal investigative mission. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other government applications and systems, with appropriate user access restrictions at the data element level and robust user auditing controls. FALCON modules, such as FALCON-DARTTS and FALCON-Roadrunner, have been deployed in support of discrete HSI mission areas and work units.

Data analyzed by the FALCON modules is aggregated and stored in the FALCON

general data storage environment. The data stored in this environment is ingested on a routine or *ad hoc* basis from other existing sources and is structured and optimized for use with the analytical tools in FALCON-DARTTS, FALCON-Roadrunner, and the other FALCON modules. For more information on the FALCON environment, please see the FALCON-Search and Analysis PIA at www.dhs.gov/privacy.

FALCON-DARTTS

As described above, in January 2014, ICE migrated the DARTTS system to the HSI FALCON environment and launched FALCON-DARTTS. FALCON-DARTTS replicates the functionality of and serves the same user groups as the legacy DARTTS system. The purpose of FALCON-DARTTS is to allow HSI investigators to generate leads for, and otherwise support, investigations of trade-based money laundering, smuggling, commercial fraud, and other crimes within the jurisdiction of HSI. FALCON-DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation. These anomalies are then independently confirmed and further investigated by HSI investigators. With the deployment of FALCON-DARTTS, the legacy DARTTS system (which included a component called "Foreign DARTTS" used by HSI's foreign law enforcement and customs partners) was retired.

ICE published a new PIA for FALCON-DARTTS on January 16, 2014, to address the migration from legacy DARTTS and to notify the public of several new system features, including (1) additional datasets and records and (2) an updated way in which datasets are physically separated. First, ICE has added to FALCON-DARTTS new financial data as well as records manually uploaded on an *ad hoc* basis, which may

include financial records, business records, trade transaction records, and transportation records.

Second, financial and law enforcement datasets analyzed by FALCON-DARTTS are maintained in the FALCON general data storage environment. In this environment, the data is aggregated with other FALCON data, and user access is controlled through a combination of data tagging, access control lists, and other technologies. Trade data (i.e., data relating to the importation and exportation of merchandise) is maintained separately in the FALCON-DARTTS trade data subsystem, which is physically and logically separate from the FALCON general data storage environment and contains different user access requirements, including requirements that export data only be used for enforcement actions involving cargo safety and security or to prevent smuggling, than the overarching FALCON-SA data storage environment. All FALCON-DARTTS users, including select foreign law enforcement and customs officials who have access to the system, access trade data through the trade data subsystem. The PIA for FALCON-DARTTS is available at www.dhs.gov/privacy.

FALCON-Roadrunner

FALCON-Roadrunner is a new system that analyzes export and financial data across large, disparate trade, financial, law enforcement, and other commercially-and publicly-available datasets. The system creates and automatically applies repeatable, analytical queries and processes to determine non-obvious, anomalous behaviors, patterns, and relationships within and across the large-scale datasets. These anomalies, patterns, and relationships provide leads that may warrant investigation for violation of U.S. export laws and regulations. Once identified, anomalies are then independently

confirmed and further investigated by HSI investigators.

FALCON-Roadrunner also supports HSI by providing export enforcement-related statistical reporting capabilities, derived from trade and financial data. These statistical functions discern, describe, and document trends within the datasets associated with proliferation, export licensing, and other export enforcement trends in order to inform ICE decision makers. The PIA for FALCON-Roadrunner is being published concurrently with this update to the DHS/ICE-005 TTAR System of Records and is available at www.dhs.gov/privacy.

Changes to Categories of Individuals, Categories of Records, Retention, and Record Sources

With the migration of DARTTS to FALCON-DARTTS and the deployment of FALCON-Roadrunner, the TTAR system of records is being modified to (1) update existing and include new categories of individuals; (2) clarify existing and include new categories of records; (3) reflect a proposed change to the retention period of the data; and (4) update the description of the record sources.

Existing categories of individuals in the DHS/ICE-005 TTAR SORN have been updated to include additional individuals. Individuals whose financial records have been lawfully obtained by law enforcement agencies during official investigations, legal processes, and/or legal settlements have been added to category (2) below; individuals identified on other denied parties or screening lists have been added to category (3) below; and individuals identified in TECS investigative records have been added to category (4) below. In addition, a new category of individuals has been added to cover applicants for U.S. visas and other individuals identified on visa applications.

Existing categories of records have been updated to clarify and simplify the description of records. Previously categorized as "customs, trade, and financial data," these records are now described separately as "trade data" and "financial data." In addition, new law enforcement records have been added, including TECS investigative records, visa security information, and trade-based and financial sanction screening lists.

The retention period for data maintained under the TTAR system of records is also being updated. Previously, data was maintained in the legacy DARTTS system for five years, archived for an additional five years, and then deleted. ICE intends to request National Archives and Records Administration (NARA) approval to retire the legacy DARTTS retention schedule. Datasets analyzed by FALCON-DARTTS and FALCON-Roadrunner will be incorporated into the forthcoming retention schedule for the FALCON environment. ICE is proposing to retain datasets used in support of FALCON-DARTTS and FALCON-Roadrunner for ten years. Some of the data analyzed by FALCON-DARTTS and FALCON-Roadrunner is already maintained in the FALCON environment and subject to a proposed retention period there; however, FALCON-DARTTS and FALCON-Roadrunner will only access these existing datasets for ten years.

Lastly, new records sources have been added as a result of the new datasets covered by this system of records. New data sources added to this system of records includes additional federal, state, and local government agencies; companies; and commercially and publicly available datasets.

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 that

have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/ICE may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

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 DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the federal government agencies collect, maintain, use, and disseminate 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 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 when 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

Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE)-005

System name:

DHS/ICE-005 Trade Transparency Analysis and Research (TTAR)

Security classification:

Sensitive But Unclassified, Law Enforcement Sensitive

System location:

Records are maintained in FALCON-DARTTS and FALCON-Roadrunner, which are IT systems owned and operated by ICE and maintained in a DHS data center. FALCON-DARTTS and FALCON-Roadrunner are accessed through the ICE Network.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

(1) Individuals who, as importers, exporters, shippers, transporters, customs 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 under the Bank Secrecy Act, or that are obtained by law enforcement agencies during official investigations, legal processes, or legal settlements;

(3) Specially Designated Nationals as defined by 31 C.F.R. § 500.306 and individuals identified on other denied parties or screening lists;

(4) Individuals identified in TECS subject records and investigative 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; and

(5) U.S. visa applicants and other individuals who are identified on the visa application (e.g., the applicant's spouse, individuals traveling with the applicant, application preparer's name, applicant's point of contact in the United States).

Categories of records in the system:

Categories of records in this system include:

(1) Biographic and other identifying information, including names; dates of birth; places of birth; Social Security numbers (SSN); Tax Identification Numbers (TIN); Exporter Identification Numbers (EINs); passport information (number and country of issuance); citizenship; nationality; location and contact information (e.g., home, business, and email addresses and telephone numbers); and other identification numbers (e.g., Alien Registration Number, driver's license number).

(2) Trade data, including trade identifier numbers (e.g., for manufacturers importers, exporters, and customs brokers) and bill of lading data (e.g., consignee names and addresses, shipper names and addresses, container numbers, carriers).

(3) Financial data, including data reported pursuant to the Bank Secrecy Act (e.g., certain transactions over $10,000) and other financial data obtained via official investigations, legal processes, or legal settlements. Financial data includes, but is not

limited to, bank account numbers, transaction numbers, and descriptions or value of financial transactions.

(4) 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) Law enforcement records, including TECS subject records and investigative records related to an ICE or CBP law enforcement matter, information obtained from the U.S. Department of Treasury's Specially Designated Nationals List, visa security information, and other trade-based and financial sanction screening lists. Law enforcement data includes, but is not limited to, names; aliases; business names; addresses; dates of birth; places of birth; citizenship; nationality; passport information; SSNs; TINs; driver's license numbers; and vehicle, vessel, and aircraft information.

(6) Other financial records, business records, trade transaction records, and transportation records associated with official law enforcement purposes.

Authority for maintenance of the system:

ICE is authorized to collect this information pursuant to 6 U.S.C. § 236; 19 U.S.C. § 1589a; the Trade Act of 2002 § 343 (Note to 19 U.S.C. § 2071); 19 U.S.C. § 1484; 50 U.S.C. app. § 2411; 19 C.F.R. §§ 161.2 and 192.14; and, 31 U.S.C. § 5316 and 31 C.F.R. 1010.340. HSI has the jurisdiction and authority to investigate violations involving the importation and exportation of merchandise into or out of the United States. Information analyzed by FALCON-DARTTS, supports, among other things, HSI's investigations into smuggling violations under 18 U.S.C. §§ 541, 542, 545, and 554; financial crimes investigations under 18 U.S.C. §§ 1956, 1957, and 1960 and the Bank Secrecy Act; and

merchandise imported in non-compliance with 19 U.S.C. §§ 1481 and 1484. Information analyzed by FALCON-Roadrunner supports, among other things, HSI's investigations into export violations – particularly those involving violations under 22 U.S.C. § 2778 and 50 U.S.C. § 1705.

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 export violations, cargo safety and security, smuggling, and related violations – including financial crimes and trade-based money laundering;

(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 data and analytical capabilities with foreign customs and law enforcement partners to further collaboration and cooperation between HSI and such officials as well as to support those officials' abilities to engage in enforcement activities involving cargo safety and security, smuggling, and related violations – including financial crimes and trade-based money laundering;

(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 Offices of the U.S. Attorneys 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 when DOJ or DHS has agreed to represent the employee; or

(4) The U.S. or any agency thereof.

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 General Services Administration 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 when 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 when DHS becomes aware of an indication of a threat or potential threat

to national or international security, or when 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 when 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 when the government has agreed to represent the employee; or

(4) the United States, when 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

(3) 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 when 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, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines 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 or 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 proposing to retain FALCON-DARTTS and FALCON-Roadrunner datasets for ten years. Some of the law enforcement data analyzed by FALCON-DARTTS and FALCON-Roadrunner is already maintained in the FALCON environment

and subject to a proposed retention period there; however, FALCON-DARTTS and FALCON-Roadrunner will only access these existing datasets for ten years.

System Manager and address:

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

FALCON-Roadrunner: Deputy Assistant Director, Counter-Proliferation Investigations Program, ICE Homeland Security Investigations, 500 12th Street, SW, Mail Stop 5109, 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 when 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 when 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, SW, 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; U.S. Department of Commerce; U.S. Department of the Treasury; U.S. Department of State; other federal, state, and local law enforcement agencies; foreign governments pursuant to international agreements or arrangements; international entities; financial institutions; transportation companies; manufacturers; customs brokers; free trade zones; port authorities; and commercially and publicly available data sources.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted portions of this system. Pursuant to exemption 5 U.S.C. § 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. § 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set

forth in those subsections: 5 U.S.C. § 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f).

Dated: November 12, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2014-28168 Filed 11/28/2014 at 8:45 am; Publication Date: 12/01/2014]