Privacy Impact Assessment
for the

FALCON Data Analysis & Research for Trade Transparency System

DHS/ICE/PIA-038

January 16, 2014

Contact Point
James Dinkins
Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
202-732-5100

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) has deployed a new information system called FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS), which is a component system of the larger HSI FALCON environment. FALCON-DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. This Privacy Impact Assessment (PIA) is necessary because FALCON-DARTTS accesses and stores personally identifiable information (PII) retrieved from data systems owned by the U.S. Department of Homeland Security (DHS) and other government agencies, and commercially available databases. It is also necessary to provide public notice of the existence of FALCON-DARTTS and to publicly document the privacy protections that are in place for the system. With the deployment of FALCON-DARTTS, the legacy DARTTS system, which served the same function as FALCON-DARTTS, as well as the PIA for legacy DARTTS will be retired.[1]

Overview

The HSI FALCON Environment

In 2012, ICE 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. In February 2012, ICE deployed the first module of FALCON with the launch of FALCON Search & Analysis (FALCON-SA). FALCON-SA provides the capability to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. FALCON-DARTTS and other FALCON modules are being deployed in support of discrete HSI mission areas and work units. For more information on the FALCON environment, please see the FALCON-SA PIA.[2] The FALCON-SA PIA Appendix is being updated to capture the FALCON-DARTTS data that is routinely ingested or uploaded on an *ad hoc* basis into FALCON-SA.

FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS)

The purpose of FALCON-DARTTS is to allow ICE 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

[1] The legacy DARTTS system is described in the DHS/ICE/PIA 006 DARTTS PIA, October 20, 2008. *See* the PIA and subsequent updates *available at* www.dhs.gov/privacy.
[2] *See* DHS/ICE/PIA-032 FALCON Search & Analysis System (FALCON-SA), *available at* www.dhs.gov/privacy.

financial data to identify statistically anomalous transactions that may warrant investigation. These anomalies are then independently confirmed and further investigated by experienced HSI investigators.

The legacy DARTTS system, which FALCON-DARTTS is replacing, used both stand-alone and web-based systems. The stand-alone DARTTS system consisted of non-networked desktop computers in participating countries. Data was updated by physically transferring the data to each machine by HSI Trade Transparency Unit (TTU) personnel. Web-based DARTTS consisted of two specific sub-systems – Enterprise DARTTS and Foreign DARTTS – that differed by the data contained within and the user base of the systems. Enterprise DARTTS, which was for U.S. government use only, contained U.S. trade and financial data, foreign trade data provided by foreign government partners, and select law enforcement data. Foreign DARTTS, which was used by authorized foreign government partners, contained only a specific country's trade data and the U.S. trade data related to that foreign partner. FALCON-DARTTS replicates the functionality of and serves the same user-groups as legacy DARTTS. With the deployment of FALCON-DARTTS, legacy DARTTS will be retired.

With the migration from the legacy DARTTS system to FALCON-DARTTS, ICE will implement enhanced user access controls and modify the way in which datasets are physically separated. Enhanced user access controls allow data access to be restricted at the record level, meaning that only datasets authorized for a user-specific profile are visible and accessible by that user.

Trade Transparency Analysis

FALCON-DARTTS is owned and operated by the HSI TTU. 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 smuggling, trafficking counterfeit merchandise, the fraudulent misclassification of merchandise, and the over- or under-valuation of merchandise to conceal the source of illicitly derived proceeds or as the means to earn illicitly derived funds supporting ongoing criminal activity. HSI will use FALCON-DARTTS to conduct trade transparency analysis to identify and investigate these illegal activities. As part of the investigative process, HSI investigators and analysts must understand the relationship between importers, exporters, and financing for a set of trade transactions, to determine which transactions are suspicious and warrant investigation. If performed manually, this process would involve hours of analysis of voluminous data. Like the system it is replacing, FALCON-DARTTS is designed specifically to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator.

FALCON-DARTTS allows HSI to perform research and analyses that are not possible in any other ICE system because of the data it analyzes and the level of detail at which the data can be analyzed. For example, FALCON-DARTTS allows investigators to view merchandise details for imports or exports and then sort on any number of variables, such as country of origin, importer name, manufacturer name, and total value. FALCON-DARTTS does not seek to predict future behavior or to "profile" individuals or entities (*i.e.*, identify individuals or entities that meet a certain pattern of behavior that has been pre-determined to be suspect). Instead, it identifies trade and financial transactions that are statistically anomalous based on user-specified queries. Investigators analyze the anomalous transactions to determine if they are in fact suspicious and warrant further investigation. If determined to warrant further investigation, HSI will gather additional facts, verify the accuracy of the FALCON-DARTTS data, and use their judgment and experience in deciding whether to investigate further. Not all anomalies lead to formal investigations.

FALCON-DARTTS allows HSI to perform three main types of analysis. It conducts international trade discrepancy analysis by comparing U.S. and foreign import and export data to identify anomalies and discrepancies that warrant further investigation for potential fraud or other illegal activity. It performs unit price analysis by analyzing trade pricing data to identify over- or under-pricing of goods, which may be an indicator of trade-based money laundering. FALCON-DARTTS also performs financial data analysis by analyzing financial reporting data forthe import and export of currency or other monetary instruments, financial transactions with financial institutions, reports of suspicious financial activities, and the identities of parties to these transactions to identify patterns of activity that may indicate trade-based money laundering schemes.

FALCON-DARTTS Data, Access, and Storage

FALCON-DARTTS analyzes three categories of data: trade data, financial data, and law enforcement data. Trade data consists of U.S. import, export, and bill of lading data as well as foreign import and export data. Financial data consists of financial transaction reports filed pursuant to the Bank Secrecy Act (BSA) provided by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and other financial data provided to HSI by federal, state, and local law enforcement agencies (see Section 2.1 for a description of this data). Law enforcement data consists of the publicly available Specially Designated Nationals (SDN) List compiled and maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), as well as subject records from U.S. Customs and Border Protection's (CBP) TECS.

FALCON-DARTTS is used by HSI Special Agents and Criminal Research Specialists who work on TTU investigations at ICE Headquarters and in the ICE HSI field and foreign attaché offices, as well as properly cleared support personnel. In addition, select CBP personnel and

foreign government partners have limited access to FALCON-DARTTS. CBP customs officers and import specialists who conduct trade transparency analyses in furtherance of CBP's mission use the trade and law enforcement datasets within FALCON-DARTTS to identify anomalous transactions that may indicate violations of U.S. trade laws. Foreign government partners that have established TTUs and have entered into a Customs Mutual Assistance Agreement (CMAA) or other similar information sharing agreements with the United States use specific trade datasets to investigate trade transactions, conduct analysis, and generate reports in FALCON-DARTTS. All ICE HSI, CBP, and foreign users of FALCON-DARTTS are able to access only data that is associated with the user's specific profile.

In FALCON-DARTTS, only ICE and CBP users are granted access to the financial and law enforcement data, which is maintained in FALCON's general data storage environment.[3] 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. Some law enforcement data used in FALCON-DARTTS analyses is already stored in the FALCON general data storage environment. Using a central data store for most FALCON data eliminates the need for multiple copies of the data. Foreign users are restricted from accessing any data that resides in the FALCON general data storage environment.

All ICE, CBP, and foreign users have access to FALCON-DARTTS trade data, which is stored outside the FALCON general data storage environment in a physically and logically separate trade data subsystem. Trade data is segregated in a separate storage environment due to its high volume and to enhance security controls for foreign users who only access trade data. Access to the subsystem is filtered through one of two web applications: (1) ICE and CBP users are granted access to all U.S. and foreign trade data via a web application that resides within the DHS/ICE network, and (2) foreign users are granted access to select trade datasets via a different web application that resides within a protected infrastructure space between the DHS Internet perimeter and the DHS/ICE network. In the trade data subsystem, foreign users are able to use the analytical tools available in FALCON-DARTTS to analyze trade data, without creating a risk of unauthorized access to or use of financial or law enforcement data.

Interaction with FALCON-SA

As FALCON-DARTTS is a component of the larger FALCON environment, select datasets in FALCON-DARTTS will be routinely ingested into and available in FALCON-SA for additional analysis and investigation using the tools available in FALCON-SA. These datasets are the publicly available SDN List as well as U.S. and foreign financial data.[4] The SDN List will be

[3] ICE users can access both financial and law enforcement datasets, while CBP users can access only the law enforcement datasets.
[4] Other datasets, such as TECS, that are already stored in FALCON's general data storage environment will also be used by FALCON-DARTTS users for analysis and investigation in FALCON-SA.

available to all FALCON-SA users for use in any investigation initiated in FALCON-SA. For financial data, however, only FALCON-SA users who are also granted FALCON-DARTTS privileges will be authorized to access the financial data via the FALCON-SA interface; other FALCON-SA users without FALCON-DARTTS privileges are unable to view, access, or analyze the FALCON-DARTTS financial data. FALCON-SA enforces these access restrictions by requiring users to designate their projects within the system as TTU investigations; otherwise, the financial datasets will not be available for use and analysis in FALCON-SA. Only FALCON-DARTTS users can initiate TTU investigations. ICE is updating the FALCON-SA PIA Appendix to reflect that the SDN List and financial data are routinely ingested into FALCON-SA.

In addition, for trade data only, ICE HSI investigators may upload, on an *ad hoc* basis, their analytical results from FALCON-DARTTS into FALCON-SA for additional analysis and investigation using the tools available in FALCON-SA. These trade results are tagged as "FALCON-DARTTS trade data" in FALCON-SA, and the user may publish the data in the system so that it is accessible by all FALCON-SA users who have been granted FALCON-DARTTS privileges. ICE is updating the FALCON-SA PIA Appendix to reflect that trade results are uploaded on an *ad hoc* basis into FALCON-SA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

ICE is authorized to collect this information pursuant to the Trade Act of 2002 § 343; 19 U.S.C. § 2071; 19 U.S.C. § 1484; and 31 U.S.C. § 5316. 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; money laundering investigations under 18 U.S.C. § 1956; and merchandise imported in non-compliance with 19 U.S.C. §§ 1481 and 1484.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN (77 Fed. Reg. 53893, Sept. 4, 2012) applies to the information maintained in FALCON-DARTTS, which is being updated separately from the publication of this PIA. FALCON-DARTTS datasets not currently listed in the TTAR SORN will be restricted from use in the system until the SORN update is published in the *Federal Register*.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan (SSP) has been completed for FALCON. The Security Authorization for FALCON was granted on January 25, 2012.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

A records retention schedule for the legacy DARTTS system was approved by NARA in 2009. With the migration to the new FALCON-DARTTS system, ICE is proposing to modify the retention periods for the data. ICE will submit a modified schedule to NARA that is consistent with the retention periods described in Section 5 below.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

ICE does not collect PII directly from individuals or enterprises for inclusion in FALCON-DARTTS. All information is provided by other government agencies and foreign governments. Forms used by other U.S. government agencies to collect information have received OMB approval pursuant to the Paperwork Reduction Act. A complete listing of other U.S. government agency forms and OMB Control numbers can be found in the Appendix (see Appendix, Table 1).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

FALCON-DARTTS Data

FALCON-DARTTS uses bulk financial and trade information collected by and received from other agencies and foreign governments (hereafter referred to as "raw data"). This raw data contains the following PII, listed by category of information:

(1) U.S. Trade Data: Names and addresses (home or business) of importers, exporters,[5] brokers, and consignees; importer IDs; exporter IDs; broker IDs; and

[5] Importers and exporters may be individuals (U.S. citizens, lawful permanent residents, or aliens), corporations, or other business entities. In some instances, the importer ID and exporter ID is the individual or entity's Social

bill of lading data (*i.e.*, data provided by carriers to confirm receipt and transportation of on-boarded cargo to U.S. Port), including consignee names and addresses, shipper names and addresses, container numbers, and carriers.

(2) Foreign Trade Data: Names of importers, exporters, and brokers; addresses of importers and exporters; importer IDs; exporter IDs; broker IDs; and manufacturer IDs.[6]

(3) Financial Data Reported Pursuant to the BSA: Names of individuals engaging in financial transactions that are reportable under the BSA (*e.g.*, certain transactions over $10,000); addresses; Social Security Numbers (SSN); Taxpayer Identification Numbers (TIN); passport numbers and country of issuance; bank account numbers; party names and addresses (*i.e.*, person making the transaction); and owner names and addresses (*i.e.*, person on whose behalf the transaction is made). BSA data is not shared with foreign partners as part of FALCON-DARTTS.

(4) Other Financial Data: U.S. and foreign financial data that has been obtained via official investigations, legal processes, and/or legal settlements (*e.g.*, addresses, SSNs, TINs, passport numbers and country of issuance, bank account numbers, transaction numbers, party names and addresses, and owner names and addresses). Other financial data is not shared with foreign partners as part of FALCON-DARTTS.

(5) Specially Designated Nationals (SDN) List:[7] A law enforcement dataset consisting of a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries as well as information about foreign individuals, groups, and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals," and their assets are blocked and U.S. persons and entities are generally prohibited from dealing with them. The SDN List is not shared with foreign partners as part of FALCON-DARTTS. The SDN List contains some or all of the following PII: individual name, business name, address, date of birth, SSN/TIN, and passport number.

Security Number or Tax Identification Number.

[6] The specific data elements received vary by country. For example, some countries provide trade data that has been stripped of PII, such as names and addresses.

[7] The SDN List is an economic and trade sanctions program operated by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). The list is 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.

(6) TECS Subject Records: TECS subject records include Person Subject, Vehicle Subject, Vessel Subject, Aircraft Subject, Thing Subject, Business Subject, and Organization Subject records.[8] Person Subject records contain PII about individuals who are the subjects of those records, such as individuals who are the targets of or witnesses in ICE HSI investigations or of immigration enforcement actions by ICE's Office of Enforcement and Removal Operations (ERO). Person Subject records may also describe individuals who are of law enforcement interest to CBP, such as those arrested by CBP for a violation of law. Some Person Subject records describe individuals who are not suspects in any law enforcement action by ICE or CBP but are seeking approval for a license, such as applicants for customs broker's licenses, or to operate a customs bonded warehouse, or be a bonded carrier, or bonded cartman. Other types of subject records may contain PII that is related to the subject records, such as a Vehicle Subject record that may contain the vehicle owner's name. TECS subject records are not shared with foreign partners as part of FALCON-DARTTS.

TECS subject records include some or all of the following PII: individual name, address, date of birth, SSN/TIN, passport number and country of issuance, bank account number(s), telephone number(s), driver's license and state of issuance, Alien Registration Number, business name, vehicle license plate, vehicle description, vessel name, vessel description, aircraft name, aircraft tail number, and aircraft description.

Ad hoc Uploads

In addition to the raw data collected from other agencies and foreign governments, ICE HSI users are permitted to manually upload records into FALCON-DARTTS on an *ad hoc* basis. Information uploaded on an *ad hoc* basis is obtained from various sources and may include financial records, business records, trade transaction records, and transportation records. For example, pursuant to an administrative customs subpoena, HSI investigators may obtain financial records from a bank associated with a shipment of goods imported into a free trade zone.

Reports Generated by FALCON-DARTTS

FALCON-DARTTS uses analytical tools to create user-driven analyses of the raw data. These analyses focus on a variety of information, such as the activities of specific individuals and entities and/or trade data for particular commodities. The specific content and format of any particular analysis varies depending on the analytical tool selected and the parameters set by the

[8] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing and DHS/CBP-011 U.S. Customs and Border Protection TECS, *available at* www.dhs.gov/privacy.

user. The analysis may include, for example, high-level graphical representations that reveal trade pricing discrepancies or itemized listings of specific transactions identified as potentially indicative of fraud or other illegal activity. ICE users of FALCON-DARTTS may publish their analytical results to the system so that other ICE users may access the results. In addition, for analyses of trade data only, ICE users may complete their analyses in FALCON-DARTTS and then import into and publish their results in FALCON-SA. Access to these analytical results in FALCON-SA is limited to FALCON-SA users who are also granted FALCON-DARTTS privileges.

2.2 What are the sources of the information and how is the information collected for the project?

All raw data analyzed by FALCON-DARTTS is provided by other government agencies and foreign governments. The specific raw data sources are:

U.S. Trade Data

(1) CBP Import Data: Import data in the forms of extracts from CBP's Automated Commercial System (ACS),[9] which CBP collects from individuals and entities importing merchandise into the United States who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via the Automated Commercial Environment.

(2) CBP Export Data: Export data in the form of Electronic Export Information[10] that CBP collects from individuals and entities exporting commodities from the United States.

(3) Bill of Lading Data: Transportation documents collected by CBP via the Automated Manifest System and provided to ICE through electronic data transfers for upload into FALCON-DARTTS.

Foreign Trade Data

(4) Foreign Import and Export Data: Import and export data provided to ICE by foreign government partners pursuant to a CMAA or other similar information sharing agreement. Certain countries provide trade data that has been stripped of PII. Other countries provide complete trade data, which includes any individuals' names and other identifying information that may be contained in the trade records.

[9] *See* DHS/CBP/PIA-003(a) CBP's Automated Commercial System (ACS)/Automated Commercial Environment (ACE)-Importer Security Filing Data, *available at* www.dhs.gov/privacy.
[10] Electronic Export Information is the export data as filed in the Automated Export System (AES). This data is the electronic equivalent of the export data formerly collected as Shipper's Export Declaration information.

Foreign trade data is loaded into the FALCON-DARTTS trade data subsystem after the foreign partner uploads the raw dataset to a secure file transfer protocol (FTP) site. ICE retrieves the data from the site and formats it before loading it into the trade data subsystem. When the data is loaded into the subsystem, it is tagged so the system knows which nation provided it and can identify that data and grant access to that government's users.

Financial Data

(5) Financial Transaction Reports filed pursuant to the BSA: The BSA, and its implementing regulations – administered by FinCEN requires financial institutions and other industries vulnerable to money laundering to take precautions against financial crime, including reporting certain financial transactions to the government. FinCEN provides FALCON-DARTTS with the following reporting data:

- Currency and Monetary Instrument Reports: declarations of currency or monetary instruments in excess of $10,000 made by persons coming into or leaving the United States.
- Currency Transaction Reports: deposits or withdrawals of more than $10,000 in currency into or from depository institutions and casinos and card clubs or any other reports filed pursuant to 31 U.S.C. § 5313 and 31 C.F.R. § 1010.311.
- Suspicious Activity Reports: information regarding suspicious financial transactions within depository institutions, money services businesses, the securities and futures industry, and casinos and card clubs or any other reports filed pursuant to 31 U.S.C. § 5318.
- Reports Relating to Coins and Currency Received in Nonfinancial Trade or Business or any other reports filed pursuant to 31 U.S.C. § 5331 and 31 C.F.R. § 1010.330.
- Reports of Foreign Bank and Financial Accounts: reports by U.S. persons who have financial interest in, or signature or authority over, foreign financial accounts in excess of $10,000 or any other reports filed pursuant to 31 U.S.C. § 5314 and 31 C.F.R. § 1010.350.

(6) Other Financial Data Provided by other Federal, State, and Local Law Enforcement Agencies: Data that has been collected by a government agency in the course of an official investigation, through legal processes, and/or through legal settlements and has been provided to ICE to deter international money laundering and related

unlawful activities. For example, a court may direct a corporation to provide data to law enforcement agencies after determining that the corporation did not practice due diligence to deter money laundering and/or has facilitated criminal activities.

Law Enforcement Data

(7) SDN List Data: The SDN List is compiled and maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and is also publically available on the OFAC website.[11]

(8) TECS Data: TECS subject records are already maintained in the FALCON general data storage environment.[12] FALCON-DARTTS leverages this data from the general environment, eliminating the need for an additional copy of the data.

Ad hoc Uploads

(9) Information uploaded on an *ad hoc* basis is obtained from various sources, such as financial institutions; transportation companies; manufacturers; customs brokers; state, local, and foreign governments; free trade zones; and port authorities.

A complete listing of other U.S. government agency forms used to collect raw data as well as the SORNs that apply to the raw data can be found in the Appendix (see Appendix, Tables 1 and 2). FALCON-DARTTS itself is the source of analyses of the raw data produced using analytical tools within the system.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. ICE and CBP users of FALCON-DARTTS use the publicly available SDN List to compare suspected trade and financial transactions against SDN List members. All commonalities identified during comparison are further researched to determine if actual links exist between the SDN List members for criminal investigative purposes.

In addition, ICE users may upload records on an *ad hoc* basis into FALCON-DARTTS that, depending on the source, contain commercial trade and/or financial data.

Lastly, commercial financial data obtained from companies by other federal, state, and/or local law enforcement agencies in the course of legal processes may also be added to FALCON-DARTTS and used for analytical purposes by ICE HSI investigators.

[11] *See* www.treasury.gov/ofac.
[12] TECS subject records are imported into the FALCON environment from the TECS law enforcement system, which is operated by CBP.

2.4 Discuss how accuracy of the data is ensured.

All raw data analyzed by FALCON-DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority. Therefore, FALCON-DARTTS relies on the systems and/or programs performing the original collection to provide accurate data. In the event that errors in raw data are discovered by FALCON-DARTTS users, the FALCON-DARTTS system owner will notify the originating agency, which will take necessary actions to determine whether an update is required.

The majority of the raw data used by FALCON-DARTTS is highly accurate because the data was collected directly from the individual or entity to whom the data pertains. Because of the law enforcement context in which FALCON-DARTTS is used; however, there are often significant impediments to directly verifying the accuracy of information with the individual to whom the specific information pertains. For example, prior to an arrest, the agency may not have any communication with the subject because of the risk of alerting the subject to the agency's investigation, which could result in the subject fleeing or altering his or her behavior in ways that impede the investigation. Since users have separate access to some of the FALCON-DARTTS source databases, as well as other databases and data sources, FALCON-DARTTS users can actually assist in identifying and correcting inaccurate information by providing a basis for users to compare existing information and determine its context. FALCON-DARTTS users receive training on the importance of verifying information from FALCON-DARTTS before including it in any analytical report or using it as the basis for any formal law enforcement action, such as arresting an individual for a crime.

For *ad hoc* uploads, users are required by policy to obtain supervisory approval before *ad hoc* data is uploaded into FALCON-DARTTS and may upload only records that are pertinent to the particular analysis project in FALCON-DARTTS in which they are working. Both the ability to upload information on an *ad hoc* basis and to access *ad hoc* data will be limited to HSI FALCON-DARTTS users only. In the event uploaded data is later identified as inaccurate, it is the responsibility of the user to remove those records from the system and re-upload the correct data. If the user who uploaded the data no longer has access privileges to FALCON-DARTTS, it is the responsibility of a supervisor or systems administrator to make the appropriate changes to the incorrect data.

All raw data analyzed by FALCON-DARTTS is updated on at least a monthly basis for all sources, or as frequently as the source system can provide updates or corrected information. A complete listing of source data refresh periods can be found in the Appendix (see Appendix, Table 3).

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that incorrect information in the raw data may be used to make decisions regarding individuals or entities.

Mitigation: This risk is mitigated by the fact that the system does not allow users to modify raw data received from the source systems, which reduces the potential for user-generated data errors. Additionally, ICE agents and investigators use the raw data only for investigative reference and lead development purposes; they will fully investigate leads generated by FALCON-DARTTS analyses before taking action against an individual or entity. To ensure they have the best evidence available to support any case they are building, the investigator will obtain information from all original data sources and further investigate the reason for the anomaly. If the anomaly can be legitimately explained, the investigator has no need to further investigate for criminal violations. Any and all information obtained from FALCON-DARTTS will be independently verified before it is acted upon or included in an ICE investigative or analytical report.

Privacy Risk: Because FALCON-DARTTS permits users to upload information on an *ad hoc* basis, it is possible for a user to, accidentally or purposefully, input incorrect or biased information into the system.

Mitigation: FALCON-DARTTS users may upload only records that are pertinent to the particular analysis project in FALCON-DARTTS on which they are working. FALCON-DARTTS automatically captures the identity of the user who uploads the information, resulting in full attribution to the user who provided it. By policy, ICE requires users to input the source name and category and the date of retrieval, which helps other users assess data quality. FALCON-DARTTS also requires supervisors to review and approve *ad hoc* uploads, thereby ensuring the data is reviewed for flaws or non-compliance with ICE policy before it is used or made available in the system. If a user provides incorrect or biased information, the information can be corrected and remedial or disciplinary action taken against the user, if appropriate. In the event uploaded data is later identified as inaccurate, it is the responsibility of the user to remove those records from the system and re-upload the correct data. If the user who uploaded the data no longer has access privileges to FALCON-DARTTS, it is the responsibility of a supervisor or systems administrator to make the appropriate changes to the incorrect data.

In addition, only ICE HSI users are permitted to add or upload information on an *ad hoc* basis to FALCON-DARTTS. CBP and foreign users are not permitted to add or upload information to FALCON-DARTTS.

Privacy Risk: There is a risk that when disparate datasets are aggregated, the use of the aggregated data will be inconsistent with the purpose for which the data was originally collected.

Mitigation: This risk is mitigated by limiting usage of FALCON-DARTTS to a very specific purpose – to identify patterns and anomalies in trade and financial data that may be indicative of criminal activity. The use of the data for this purpose is consistent with the original purpose for which it was collected – to regulate trade and enforce U.S. import-export and financial criminal laws.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

ICE Use of FALCON-DARTTS

ICE users of FALCON-DARTTS conduct analyses of raw trade and financial data to identify potential violations of U.S. and foreign criminal laws. The analyses are designed to generate leads for and assist with the investigation of trade-based money laundering, contraband smuggling, and trade fraud. FALCON-DARTTS conducts three types of analyses:

(1) International Trade Discrepancy Analysis: U.S. and foreign import/export data is compared to identify anomalies and discrepancies that warrant further investigation for potential fraud or other illegal activity.

(2) Unit Price Analysis: Trade pricing data is analyzed to identify over- or under-valuation of goods, which may be indicative of trade-based money laundering or other import-export crimes.

(3) Financial Data Analysis: Financial reporting data (the import/export of currency, financial transactions with financial institutions, reports of suspicious financial activities, and the identities of parties to these transactions) is analyzed to identify patterns of activity that may indicate money laundering schemes.

In addition, the law enforcement data within FALCON-DARTTS is used to (1) determine whether an entity being researched as a result of trade and financial data analysis is already part of a pending ICE HSI investigation or was involved in an investigation that is now closed and (2) identify international trade and/or financial transactions that are associated with a specially-designated individual or entity, which allows ICE HSI to take appropriate investigative actions in a timely and more efficient manner.

ICE HSI investigators with experience conducting financial crimes and trade fraud investigations use the completed FALCON-DARTTS analyses to identify possible criminal activity and provide support to field investigations. Depending on their specific areas of responsibility, HSI investigators may use the analyses for one or more purposes. HSI investigators at ICE Headquarters refer the results of FALCON-DARTTS analyses to HSI field offices as part

of an investigative referral package to initiate or support a criminal investigation. All referrals to the field are documented in official reports of investigation or intelligence reports intended for the exclusive use of HSI investigators. HSI investigators in domestic field offices may also independently generate leads and subsequent investigations using FALCON-DARTTS analyses. HSI investigators in attaché offices at U.S. Embassies abroad use the analyses to respond to inquiries from foreign partner TTUs. If a foreign TTU identifies suspicious U.S. trade transactions of interest, HSI investigators will validate that the transactions are, in fact, suspicious, and ICE will coordinate joint investigations on those specific trade records. ICE may also open its own investigation into the matter.

To enhance their FALCON-DARTTS analysis of trade data, HSI investigators may, on an *ad hoc* basis, import into and publish their analytical results in FALCON-SA for additional analysis and investigation using the tools and additional data available in FALCON-SA. Trade results that are imported into FALCON-SA are tagged as "FALCON-DARTTS trade data" and are published in in FALCON-SA so they are accessible by all other FALCON-SA users who are also granted FALCON-DARTTS privileges. Only trade results, not searchable bulk trade data, are ingested into and available in FALCON-SA. ICE is updating the FALCON-SA PIA Appendix to reflect that trade results are uploaded on an *ad hoc* basis into FALCON-SA.

Similarly, HSI investigators may access U.S. and foreign financial data from FALCON-DARTTS in FALCON-SA to conduct additional analysis and investigation using the tools and additional data available in FALCON-SA. These datasets are routinely ingested into FALCON-SA, and only FALCON-SA users who are also granted FALCON-DARTTS privileges will be authorized to access the financial data via the FALCON-SA interface. ICE is updating the FALCON-SA PIA Appendix to reflect that financial data is routinely ingested into FALCON-SA.[13]

[13] The FALCON-SA PIA Appendix is also being updated to reflect the addition of the publically available SDN List as a routine ingest. The SDN List will be available to all FALCON-SA users for use in any investigation initiated in FALCON-SA.

A table listing of the sources, types, and ICE uses of FALCON-DARTTS data is included below.

ICE Uses of Information

Sources of Information	Personally Identifiable Information	Uses of Information
Trade Data		
CBP; foreign government partners	Name Address Trade ID number (*e.g.*, importer ID)	Used to identify individuals who are involved in a transaction if a criminal violation involving cargo safety and security or smuggling is suspected. Used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects.
Financial Data		
FinCEN; other financial data	Name Address	Used to identify the people involved in a transaction if a criminal violation is suspected. Used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects.
	SSN/TIN; Trade ID number (*e.g.*, importer ID)	Used as unique identifier of an individual. For example, in FALCON-DARTTS analysts can use a SSN as one of the parameters in a search and potentially find SSNs that are associated with more than one person. Analysts can also identify the minimum number of names associated with a SSN and identify which SSNs are associated with a minimum or maximum dollar amount. The results of these searches can lead to the discovery of potential criminal violations. Used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects.
	Passport number	Used in a similar way as SSNs, passport numbers are generally unique to an individual and are used to identify individuals
	Bank account number	Identifies the bank or depository institution and the person involved in the transaction. Used to conduct link analysis to identify relationships that

		may help identify suspect transactions, witnesses, or suspects.
Law Enforcement Data		
CBP	Name; address; date of birth; SSN/TIN; passport number and country of issuance; bank account number(s); telephone number(s); driver's license number and state of issuance; Alien Registration Number; business name; vehicle license plate and description; vessel name and description; aircraft name, tail number, and description	Used to determine whether an entity being researched in FALCON-DARTTS is already part of a pending ICE HSI investigation or was involved in an investigation that is now closed.
OFAC	Name; business name; address; date of birth; SSN/TIN; passport number	Used to identify international trade and/or financial transactions that are associated with a specially-designated individual or entity

CBP Use of FALCON-DARTTS

CBP customs officers and import specialists use FALCON-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. Specifically, CBP personnel use FALCON-DARTTS trade and law enforcement datasets[14] to identify anomalous transactions that may indicate violations of U.S. trade laws. If ICE elects not to open an investigation into these transactions, CBP may initiate administrative enforcement actions to recover delinquent revenue or penalties. Before initiating a formal administrative action, CBP first follows up on the anomalous transactions to determine if they are in fact suspicious and warrant further inquiry. CBP personnel will gather additional facts, verify the accuracy of the FALCON-DARTTS data, and use their judgment and experience in making the determination. Not all anomalous or suspicious transactions identified in FALCON-DARTTS will lead to CBP administrative actions.

Foreign Partner Use of FALCON-DARTTS

Foreign government partners that have established TTUs and have entered into a CMAA or other similar information sharing agreement with the United States, and are granted access to the trade data subsystem of FALCON-DARTTS, use the subsystem to conduct similar analyses as those described in this PIA. Foreign users who have access to FALCON-DARTTS are granted a user role that allows them to use only the trade data provided by their country and the related U.S. trade data[15] to investigate trade transactions, conduct analysis, and generate reports.

[14] CBP users do not have access to the financial datasets.
[15] Foreign users do not have access to the financial and law enforcement datasets or the trade datasets of other partner countries, unless access to other partner countries' data is authorized pursuant to information sharing

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. In response to user-specified queries, FALCON-DARTTS uses technology to assist its users in identifying suspicious trade transactions by analyzing trade and financial data and identifying data that is statistically anomalous. Such anomalies can indicate trade-based money laundering or other import-export crimes that ICE HSI is responsible for investigating, such as smuggling, trafficking of counterfeit merchandise, the fraudulent misclassification of merchandise, and the over- or under-valuation of merchandise to conceal the source of illicitly derived proceeds or as the means to earn illicitly derived funds supporting ongoing criminal activity. For example, FALCON-DARTTS allows HSI investigators to view totals for merchandise imports and sort on any number of variables, such as country of origin, importer name, manufacturer name, and total value. Investigators follow up on anomalous transactions to determine whether they are in fact suspicious and warrant further investigation. Not all anomalies lead to formal investigations.

FALCON-DARTTS can also identify links between individuals and/or entities based on commonalities, such as identification numbers, addresses, or other information. These commonalities in and of themselves are not suspicious, but in the context of additional information, they can assist investigators in identifying potentially criminal activity and lead to identification of witness, other suspects, or additional suspicious transactions.

3.3 Are there other components with assigned roles and responsibilities within the system?

In addition to ICE HSI personnel, select CBP personnel and foreign government partners have limited access to FALCON-DARTTS. CBP customs officers and import specialists who conduct trade transparency analysis in furtherance of CBP's mission have access to the trade and law enforcement datasets available in FALCON-DARTTS to identify anomalous transactions that may indicate violation of U.S. trade laws. Because the scope of CBP's law enforcement authority is not as broad as ICE HSI, CBP personnel are assigned more restricted user roles in the system. Specifically, CBP users are not granted access to any financial datasets in FALCON-DARTTS.

Foreign government partners that have established TTUs and have entered into a CMAA or other similar information sharing agreement with the United States are granted access to specific trade datasets to investigate trade transactions, conduct analysis, and generate reports in the FALCON-DARTTS trade data subsystem. Foreign users do not have access to the FALCON-

agreements.

DARTTS financial and law enforcement datasets stored in the FALCON general environment. Foreign users are able to access only the trade data related to their country and the related U.S. trade transactions, unless access to other partner countries' data is authorized via information sharing agreements.

All ICE HSI, CBP, and foreign users of FALCON-DARTTS are able to access only data that is associated with the user's specific profile.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to or unauthorized use of the information maintained in FALCON-DARTTS.

Mitigation: As described in Section 8.3, security and access controls are in place to mitigate the risk of unauthorized individuals gaining access to PII. Access to FALCON-DARTTS is limited to users who conduct official trade transparency investigative activities. Foreign user access is limited to U.S. and select foreign trade data maintained in the FALCON-DARTTS trade data subsystem, with no access to the financial and law enforcement datasets stored in the FALCON environment or any other internal network resources. In addition, all FALCON-DARTTS users must complete system training that covers the appropriate uses of system data, disclosure and dissemination of records, and system security. ICE or CBP personnel who are found to access or use the FALCON-DARTTS data in an unauthorized manner will be disciplined in accordance with DHS policy. Foreign users are removed from the system by ICE HSI TTU and may be subject to disciplinary action by their foreign government employer. These and other controls described in this PIA ensure the system is used only by authorized users for the intended purpose.

Additionally, any law enforcement investigation that is initiated as a result of a FALCON-DARTTS analysis will, from that point forward, be carried out like any other criminal investigation. Normal investigatory protocols will be followed and the same civil liberty and constitutional restrictions, such as the Fourth Amendment's probable cause requirements, will apply. ICE HSI investigators will fully investigate leads generated by FALCON-DARTTS analysis before taking action against an individual or entity. To ensure they have the best evidence available to support any case they are building, the investigator will obtain information from all original data sources and will further investigate the reason for the anomaly. If the anomaly can be legitimately explained, such as when the anomaly is an administrative error or is part of a legal business process, the investigator has no need to further investigate for criminal violations. Any and all information obtained from FALCON-DARTTS will be independently verified before it is acted upon or included in an ICE investigative or analytical report.

Privacy Risk: There is a risk that FALCON-DARTTS users will use the system tools and data for purposes beyond what is described in this PIA.

Mitigation: The risk of system misuse is minimized as user rights for FALCON-DARTTS are limited to personnel with a need to know, specifically only ICE and CBP personnel and foreign partners involved with financial and trade investigations. User rights are granted on a requirements basis, meaning that users will be granted only the system functionality required of their position. In addition, FALCON-DARTTS has a robust auditing feature that helps to identify and support accountability for user misconduct. User activity is audited heavily, including actions such as uploading records or data, extracting information from the system, resolving entities, searches, and viewing records. ICE HSI has established controls that are based in policy, and when possible enforced by technology, that provide clear instruction on what the authorized uses of the system are. Disciplinary action for violations of HSI policies regarding the system is taken when warranted. Before receiving access to the system, all users are trained on system use and other policies governing the system. Lastly, FALCON-DARTTS access controls are highly customizable and can be set at the record or even data field level. This ensures that users without a need to know are technically barred from accessing that information. Section 8.1 contains an in-depth discussion of all controls that help to ensure the system and its information are used in accordance with the practices stated in this PIA.

Privacy Risk: There is a risk that the FALCON-DARTTS financial data that is routinely ingested into FALCON-SA will be used for unauthorized purposes in FALCON-SA.

Mitigation: FALCON-SA prohibits users from viewing, using, or analyzing the financial data in FALCON-SA unless those users already have privileges to use the data in FALCON-DARTTS. System-enforced access restrictions protect the financial data that is routinely ingested into FALCON-SA by requiring users with FALCON-DARTTS privileges to designate their projects as TTU investigations; otherwise, the financial datasets will not be available for use in the analysis or investigation. Users must explicitly select that they want to conduct a TTU investigation to have access to FALCON-DARTTS financial datasets in FALCON-SA.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

For *ad hoc* uploads, depending on the method of collection (*e.g.*, subpoena), individuals may be made aware that their information is being collected by a government agency for a law enforcement purpose. These individuals, however, are not likely to be aware that their information is used in FALCON-DARTTS. For raw data, ICE does not collect information directly from

individuals or entities for use in FALCON-DARTTS, and therefore, is not in a position to provide notice at the time of collection. The U.S. and foreign government agencies that collect this information are responsible for providing appropriate notice, either on the forms used to collect the information and/or through other forms of public notice, such as Privacy Act System of Records Notices (SORN). A complete listing of the SORNs that apply to the raw data ICE receives from U.S. agencies for use in FALCON-DARTTS can be found in the Appendix (see Appendix, Table 2).

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The raw data analyzed by FALCON-DARTTS is collected by other government agencies. The information collected by other U.S. agencies is required by U.S. law to be provided to these agencies. For example, individuals and corporations may choose to not import or export goods, but should they choose to undertake such trade activities, they must submit required information to the appropriate U.S. agency. Furthermore, for raw data or *ad hoc*-uploaded information that is collected in the course of a law enforcement process, there may be no opportunity for individuals to consent, decline, or to opt out of the collection of their information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may be unaware that their information is contained within FALCON-DARTTS.

Mitigation: Publication of this PIA and the TTAR SORN mitigates this risk by providing a detailed description of the types of individuals whose information is contained within the system and the types of trade and financial transactions that make up FALCON-DARTTS data.

Because FALCON-DARTTS is a system used for criminal law enforcement purposes, notice or the opportunity to consent to use of the information would compromise the underlying law enforcement purpose of the system and may put pending investigations at risk. In addition, ICE does not directly collect the trade and financial data but receives the data from other U.S. and foreign government agencies. ICE is not, therefore, in a position to provide notice or an opportunity to obtain consent from the individuals and entities from whom this information is collected. For that reason, specific notice and the opportunity to consent to these specific uses are not provided.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

ICE intends to request National Archives and Records Administration (NARA) approval to retire the legacy DARTTS records retention schedule and incorporate the retention periods for data maintained in FALCON-DARTTS into the forthcoming records schedule for the FALCON environment. With this change, ICE will request to retain the FALCON-DARTTS datasets, including the data in the trade data subsystem, for ten years in the system, which is a change from the legacy DARTTS retention policy of five years in the system and five years in an archive. While the total retention period would not change, this proposal will result in the FALCON-DARTTS data remaining available to users in the system for an additional five years. This change in retention policy is being requested to enhance the performance of the FALCON-DARTTS system by having more data in the system spanning a longer period of time. With this expanded data set, ICE expects to be able to better identify suspicious transactions that are part of a longer-term conspiracy or more sophisticated criminal activity and help identify parties that would not otherwise be implicated or help identify innocent parties.

ICE will also propose to lengthen the retention period for the "inputs" to the FALCON-DARTTS system (*i.e.*, the original raw data imported into FALCON-DARTTS from the source systems) so that it matches the retention period for the production data used in FALCON-DARTTS. Currently, the retention policy for the inputs is five years. ICE is proposing to change the retention period for all FALCON-DARTTS inputs to ten years. This ten-year retention period will apply to all routinely ingested U.S. and foreign data as well as records that are uploaded on an *ad hoc* basis into FALCON-DARTTS by ICE HSI users. The expanded retention period is necessary so that the inputs are retained for the same length of time as the data in the FALCON-DARTTS system, in case they are needed for data integrity and system maintenance/recovery purposes. Data that is archived is not kept in sync with its source system, which would introduce a risk of data inaccuracy if data needed to be pulled from the archive and reintroduced for use in the system.

If an underlying source system deletes or changes its data, FALCON-DARTTS will also delete or change its data during its next refresh from the source system. A complete listing of source data refresh periods can be found in the Appendix (see Appendix, Table 3).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in FALCON-DARTTS will be retained for longer than necessary given the purpose of the system and the original reason the information was collected.

Mitigation: The ten year retention period proposed for FALCON-DARTTS, including data in the trade data subsystem, is appropriate for the purpose of the system, which is to analyze current and historical trade and financial information to identify patterns and anomalies that may

indicate criminal activity. Investigators typically do not need to access and analyze data that is more than ten years old to conduct the types of analyses described in this PIA. Given the nature of TTU investigations (*i.e.*, investigations concerning long-term or more sophisticated criminal activity), ten years of data can help identify parties that would not otherwise be implicated or help identify innocent parties. For example, ICE may use as a basis for its criminal cases CBP trade data on administrative penalties, which are issued to individuals and entities by CBP for compliance issues with trade requirements. A CBP penalty case may, years after the penalty was issued, ultimately result in a determination that the individual or entity made administrative errors, and the penalty is overturned. At the outcome of the case, CBP trade data is updated, and thus, FALCON-DARTTS trade data is updated, to reflect that the penalty was overturned. The ten year retention for FALCON-DARTTS data ensures that sufficient and up-to-date information is available to conduct meaningful analyses for law enforcement purposes, while not keeping the information for any longer than is necessary or in a way that is inconsistent with the original purpose of the collection.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Foreign government partners are granted access to only trade data within the physically and logically separate trade data subsystem of FALCON-DARTTS. Access is limited to the trade data of their country and the related U.S. trade transactions between their country and the United States, unless access to other partner countries' data is authorized via information sharing agreements. Foreign partners use this trade data to investigate trade transactions, conduct analysis, and generate reports.

As described in the Overview, the FALCON-DARTTS trade data subsystem is configured to ensure that foreign users access only the select trade datasets they are authorized to view, access, and analyze in the subsystem, with no access beyond that to the financial and law enforcement datasets stored in the FALCON environment or any other internal network resources. Foreign access to the physically and logically separate trade data subsystem is filtered through a web application that resides within a protected infrastructure space between the DHS Internet perimeter and the DHS/ICE network. This protected infrastructure space is known as a network DMZ (demilitarized zone). The separation of trade data from other FALCON-DARTTS datasets reduces

the risk of unauthorized access to or use of financial or law enforcement data by foreign users of the system.

In addition to sharing with foreign governments, FALCON-DARTTS analytical results may be shared outside of DHS with other federal, state, local, and foreign agencies for law enforcement investigatory purposes on a case-by-case basis consistent with the purpose for which the data was collected. ICE only shares this information after the underlying data has been validated and only for law enforcement or homeland security purposes. This sharing will take place only after DHS determines that the receiving component or agency has a need-to-know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in the DHS/ICE-005 TTAR SORN and any other applicable laws, regulations, or directives.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The TTAR SORN applies to FALCON-DARTTS information and includes routine uses that permit external sharing for law enforcement, homeland and national security, audit, congressional, data breach, litigation, and records management purposes. The SORN also permits the sharing of U.S. trade data with foreign governments pursuant to CMAAs or other similar agreements to further the identification and prosecution of trade-based money laundering, smuggling, and trade fraud. All external sharing is compatible with the law enforcement purpose for which ICE originally compiled and used this information.

6.3 Does the project place limitations on re-dissemination?

Re-dissemination of FALCON-DARTTS information by an external agency is not permitted unless the agency has received ICE's express authorization (*i.e.*, third agency rule). However, by agreement with certain agencies that provide data to ICE, ICE received advance authorization to share their information with specified third parties and/or for specified purposes.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

By policy and via user training, users are instructed to record any disclosure of information from FALCON-DARTTS outside of DHS by completing an accounting for disclosure form in FALCON-DARTTS. The form captures the date, nature, and purpose of the disclosure and the recipient's contact information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data will be shared with external parties lacking a need to know, and that external sharing will not be properly recorded as required by the Privacy Act.

Mitigation: FALCON-DARTTS users are required by law and policy, which is reinforced by user training, to share information from FALCON-DARTTS with only those external partners who have a law enforcement, intelligence, or national security need-to-know. This requirement is in keeping with the law enforcement purpose of the system and the scope of ICE's mission as a law enforcement agency. Users are required to complete an online form in the system when making an external disclosure to comply with the provisions of the Privacy Act, 5 U.S.C. § 552a(c).

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any record contained in FALCON-DARTTS, or seeking to contest its content, may submit a request in writing to ICE FOIA Officer, by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(866) 633-1182
http://www.ice.gov/foia/.

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in FALCON-DARTTS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. See 74 Fed. Reg. 38887 (Aug. 5, 2009).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The correction procedures are identical to those described in Section 7.1 above. All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in FALCON-DARTTS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of

DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. See 74 Fed. Reg. 38887 (Aug. 5, 2009).

7.3 How does the project notify individuals about the procedures for correcting their information?

The information about correction is made available through the publication of this PIA and the associated SORNs. Because FALCON-DARTTS contains copies of datasets owned by DHS components and offices or other agencies, individuals may also have the option to seek access to and correction of their data directly from those agencies or offices that originally collected it. Information that is corrected in the original source system will be updated in the FALCON-DARTTS data repository during routine refreshes thereby ensuring accurate and current information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to meaningfully participate in the use of their data as maintained in this system, or determine whether the system maintains records about them.

Mitigation: Because the data in this system originates from other systems of records with a law enforcement purpose, individuals' rights to be notified of the existence of data about them, and to direct how that data may be used by ICE HSI, are limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

As mentioned before, FALCON-DARTTS is a component system of the larger ICE HSI FALCON environment. As a result, FALCON-DARTTS uses the same access controls, user auditing, and accountability as those described in the FALCON-SA PIA. For example, user access controls allow data access to be restricted at the record level, meaning that only datasets authorized

for a user-specific profile are visible and accessible by that user. Audit capabilities log user activities in a user activity report, which is used to identify users who are using the system improperly. For more information on these controls, auditing, and accountability, please see the FALCON-SA PIA.

In addition to the auditing and accountability functions leveraged from FALCON-SA, FALCON-DARTTS will maintain an additional audit trail with respect to its compliance with the July 2006 Memorandum of Understanding with the U.S. Department of the Treasury's FinCEN to identify, with respect to each query, the user, time and nature of the query, and the BSA information viewed.

Furthermore, all ICE HSI, CBP, and foreign users are subject to data download restrictions, thus limiting the amount of information they can pull from FALCON-DARTTS and the trade data subsystem. Users are notified of a pre-determined data limit set by the FALCON-DARTTS Administrator that cannot be exceeded on a monthly basis. Technical controls within the system prohibit users from exceeding this data limit. The data download restrictions help minimize the risk that a user could extract excessive bulk data from FALCON-DARTTS for illicit purposes.

Lastly, as described in the Overview and Section 6.1, the FALCON-DARTTS trade data subsystem is configured to ensure that foreign users access only the select trade datasets they are authorized to view, access, and analyze in the subsystem, with no access to the financial and law enforcement datasets stored in the FALCON environment or any other internal network resources. Foreign access to the physically and logically separate trade data subsystem is filtered through a web application that resides within a protected infrastructure space between the DHS Internet perimeter and the DHS/ICE network. The separation of trade data from other FALCON-DARTTS datasets reduces the risk of unauthorized access to or use of financial or law enforcement data by foreign users.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

In addition to taking the FALCON-SA training, which is described in the FALCON-SA PIA, ICE and CBP users receive FALCON-DARTTS training. This training includes the users signing the FALCON-DARTTS rules of behavior, appropriate uses of system data, disclosure and dissemination of records, and system security. Users must complete all training in order to receive authorization to access FALCON-DARTTS. All personnel who have access to the ICE network are also required to take annual privacy and security training, which emphasizes the DHS Rules of Behavior and other legal and policy restrictions on user behavior.

Foreign users do not receive training on the FALCON-SA system, since they are not granted access to the data or the tools and functionality within FALCON-SA. They are, however, required to complete training specific to the FALCON-DARTTS trade data subsystem that covers

appropriate uses of system data, disclosure and dissemination of records, and system security. Foreign users must complete this system training and sign the FALCON-DARTTS foreign user agreement before being granted access to trade data within the trade data subsystem.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only ICE HSI, CBP, and foreign government personnel who require access to the functionality and data available in FALCON-DARTTS and its trade data subsystem as part of the performance of their official duties will be granted access. Access is granted on a case-by-case basis by the FALCON-DARTTS Administrator, who is designated by the TTU Unit Chief. User roles are reviewed regularly by a FALCON-DARTTS ICE Supervisor to ensure that users have the appropriate access and that users who no longer require access are removed from the access list. All ICE HSI, CBP, and foreign users of FALCON-DARTTS are able to access only data that is associated with the user's specific profile.

To be considered for access to the system, an ICE HSI employee must complete a User Agreement for FALCON-DARTTS, and the employee's supervisor must validate that the employee has a job-related need-to-know and determine what user role should be assigned. Supervisors submit a FALCON-DARTTS User Agreement to a designated point of contact (POC) who validates that the employee meets all requirements for access to the system, such as the appropriate level of background check. Once this is verified, the FALCON-DARTTS POC notifies the FALCON-DARTTS Administrator to create the user account and the associated job-related user role that should be assigned. For personnel assigned to ICE on a task force or from other agencies, the same process is followed. In addition, any applicable agreement governing the task force or assignment is reviewed to ensure compliance. For contractors, a government employee overseeing the contract will submit user requests and perform the other supervisory roles above.

CBP personnel follow the same user access process as ICE HSI personnel. Because the scope of CBP's law enforcement authority is not as broad as the authority held by ICE HSI, however, CBP personnel are assigned more restricted user roles in the system. Specifically, CBP users are authorized to access only trade and law enforcement data, but not financial data, in FALCON-DARTTS.

Foreign users, who may be granted access to only select trade datasets stored in the FALCON-DARTTS trade data subsystem with no access beyond that to the financial and law enforcement datasets stored in the FALCON environment, are vetted by the ICE attaché office in the foreign user's country before they are considered for access to the subsystem. User accounts are approved by the FALCON-DARTTS Administrator; foreign governments do not have the authority to create or modify user accounts or privileges. Foreign users must sign the FALCON-

DARTTS foreign user agreement before being granted access to trade data within the trade data subsystem.

Currently FALCON-DARTTS has six user roles:

(1) FALCON-DARTTS ICE User: Investigates financial or trade transactions, conducts analysis, and generates reports.

(2) FALCON-DARTTS CBP User: Identifies trade transaction discrepancies, conducts analysis, and generates reports.

(3) FALCON-DARTTS Foreign User: Investigates trade transactions, conducts analysis, and generates reports.

(4) FALCON-DARTTS ICE Supervisor: Investigates financial or trade transactions, conducts analysis, generates reports, and assigns user roles.

(5) FALCON-DARTTS ICE Administrator: Creates, activates, revokes, and/or removes user access and accounts.

(6) FALCON-DARTTS ICE System Owner: Investigates financial or trade transactions, conducts analysis, generates reports, assigns user roles, and performs user and activity auditing.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

ICE established a governance process to monitor the ongoing operations of the FALCON environment, to decide requests to add new data sources to the system, to expand user privileges to other DHS components or other agencies, and to establish policies and procedures that govern system operation and user behavior. The governance process is staffed by ICE HSI leadership and senior managers, and advisory services are provided by the Office of Principal Legal Advisor and the ICE Privacy and Records Office.

The existence of this governance process will help ensure that any proposals for new data sharing arrangements are appropriately vetted for legal and privacy risks as well as compliance with the DHS Fair Information Practice Principles. In addition, formal written agreements between ICE and other agencies to share data or provide access to FALCON-DARTTS will be reviewed by the ICE Privacy and Records Office and Office of Principal Legal Advisor as a matter of routine. All information contained within FALCON-DARTTS, including the trade data subsystem accessed by foreign users, is subject to the governance process listed above.

Responsible Officials

Lyn Rahilly, Privacy Officer
U.S. Immigration & Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Table 1. Trade Data and Financial Transactions Forms

Types of Forms	Form
Trade Data Forms	U.S. Customs and Border Protection Form 7501 – Entry Summary, OMB Control No. 1651-0022
	Electronic Export Information filed electronically through the Automated Export System (AES), OMB Control No. 0607-0152
	Cargo inventory and carrier manifest information filed electronically through the Automated Manifest System (AMS), OMB Control No. 1651-0001
Financial Transaction Forms	FinCEN Form 101 – Suspicious Activity Report by Securities and Futures Industries, OMB Control No. 1506-0019
	FinCEN Form 102 – Suspicious Activity Report by Casinos and Card Clubs, OMB Control No. 1506-0006
	FinCEN Form 103 – Currency Transaction Report by Casinos and Card Clubs, OMB Control No. 1506-0005
	FinCEN Form 104 – Currency Transaction Report, OMB Control No. 1506-0004
	FinCEN Form 105 – Report of International Transportation of Currency or Monetary Instruments, OMB Control No. 1506-0014
	FinCEN Form 109 – Suspicious Activity Report by Money Services Business, OMB Control No. 1506-0015
	FinCEN Form 8300 – Report of Cash Payments Over $10,000 Received in a Trade or Business, OMB Control No. 1506-0018
	Treasury Form TD-F 90-22.47 – Suspicious Activity Report by Depository Institutions, OMB Control No. 1506-0001
	Treasury Form TD-F 90-22.1 – Report of Foreign Bank and Financial Accounts, OMB Control No. 1545-2038

Table 2. Privacy Act System of Records Notices

Agency	Systems of Records Notices
U.S. Immigration and Customs Enforcement	Student Exchange and Visitor Information System (SEVIS) (DHS/ICE-001)
U.S. Customs and Border Protection (CBP)	Automated Commercial System (ACS) (Treasury/CS.278)
	Automated Commercial Environment/International Trade Data System (ACE/ITDS) (DHS/CBP-001)
	TECS (DHS/CBP-011)
	Suspicious Activity Report System (Treasury/FinCEN.002)

U. S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN)	Bank Secrecy Act Reports System (Treasury/FinCEN.003)

Table 3. Source Data Refresh Periods

Sources of Information	Category of Information	Refresh Period
Trade Data		
CBP	Automated Commercial System (ACS) Import Data	Daily
	Automated Export System (AES) Export Data	
	Automated Manifest System (AMS) Bill of Lading Data	
Foreign Government Partners	Foreign Trade Data	Monthly
Financial Data		
FinCEN	BSA Data	Every 10 days
Other Federal, State, and Local Law Enforcement Agencies	Other Financial Data	When obtained
Law Enforcement Data		
U.S. Department of the Treasury Office of Foreign Assets Control (OFAC)	SDN List	Monthly
CBP	TECS Subject Records	Daily
Student Exchange and Visitor Data		
ICE	SEVIS Records	Daily
***Ad hoc* Uploads**		
Various sources, such as financial institutions, transportation companies, manufactures, customs brokers, state, local, and foreign governments, free trade zones, and port authorities	Financial records, business records, trade transaction records, and transportation records	When obtained