Privacy Impact Assessment
for the

Data Analysis & Research for Trade Transparency System (DARTTS)

April 26, 2010

Contact Point
James A. Dinkins, Director
Office of Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) operates the Data Analysis and Research for Trade Transparency System (DARTTS), which supports ICE investigations of trade-based money laundering, contraband smuggling, and trade fraud. DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. These anomalies are then independently confirmed and further investigated by experienced ICE investigators. The original Privacy Impact Assessment (PIA) for DARTTS was published in October 2008. ICE is migrating DARTTS to the ICE Enterprise Network, and has added two new sets of financial data and a new set of trade data. ICE also implemented new audit features and capabilities to enhance integrity and accountability. ICE is updating and republishing the DARTTS PIA to reflect these changes.

Overview

Background

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 ICE is responsible for investigating, such as contraband smuggling, trafficking of counterfeit goods, misclassification of goods, and the over- or under-valuation of goods to hide the proceeds of illegal activities.

DARTTS is owned and operated by the ICE Office of Investigations (OI) Trade Transparency Unit (TTU) and is used to investigate these illegal activities. As part of the investigative process, ICE investigators and analysts must understand the relationship between importers and exporters and the financing for a set of trade transactions to determine which transactions are suspicious and warrant investigation. If performed manually, this process often involves hours of analysis of voluminous data. DARTTS is specifically designed to make this investigative process more efficient by automating the analysis and the identification of anomalies for the investigator.

DARTTS Updates

This update to the DARTTS PIA, originally published in October 2008, includes enhancements to the DARTTS system and the incorporation of new financial and trade data described below:

- Transition from a stand-alone network to the ICE Enterprise Network to support enhanced system functionality and expanding access to TTU personnel in the field. Stand-alone workstations will remain in operation in attaché offices at U.S. embassies abroad until ICE can transition them to the ICE Enterprise Network as well.
- Incorporation of two new financial data sets received from the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN): (1) Suspicious Activity Reports

from casinos, card clubs, and money services businesses[1], and (2) financial data provided in the Report of Foreign Bank and Financial Accounts[2].

- Incorporation of new trade data received from the U.S. Customs and Border Protection (CBP) Automated Manifest System pertaining to electronic cargo inventory and carrier manifest information (also known as "bill of lading" data).
- Implementation of new auditing features within DARTTS to provide a more detailed audit trail of user activity and enhance the overall integrity and accountability of the system.

DARTTS Capabilities

DARTTS allows ICE to perform research and analyses that are not available in any other system because of the data it contains and the levels of detail at which the data can be analyzed. For instance, DARTTS allows investigators to view totals for merchandise imports and then sort on any number of variables, such as country of origin, importer name, manufacturer name, and total value. 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 known facts and user queries.

Investigators further research anomalous transactions to determine if they are in fact suspicious and warrant further investigation. Investigators gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination. Not all anomalies lead to formal investigations.

In response to user-specified queries, DARTTS can also conduct "link analysis," which identifies links (relationships) between individuals and/or entities based on commonalities, such as identification numbers, addresses and names. These commonalities in and of themselves are not suspicious, but in the context of additional information they may help investigators identify potentially criminal activity, suspicious transactions, witnesses, or suspects.

Information Sources

DARTTS uses trade data collected by U.S. Customs and Border Protection (CBP), U.S. Bureau of Census within the U.S. Department of Commerce, and foreign governments, and financial data collected by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). DARTTS data is primarily related to international commercial trade and financial transactions. DARTTS does not allow ICE investigators to obtain any data they couldn't otherwise access in the course of their investigative activities. In addition, DARTTS does not allow users to modify or append the data. DARTTS is maintained on the ICE Enterprise Network and on stand-alone workstations used by ICE

[1] Money services businesses are required by the Bank Secrecy Act to complete and submit Suspicious Activity Reports to FinCEN. They include money transmitters; issuers, redeemers and sellers of money orders and travelers' checks; and check cashers and currency exchangers.

[2] Reports of Foreign Bank and Financial Accounts pertain to individuals who have a financial interest in, or signature authority, over any financial accounts, including bank, securities, or other types of financial accounts in a foreign country, if the aggregate value of these financial accounts exceeds $10,000.

investigators in attaché offices at U.S. embassies abroad. Notice of the existence and operation of DARTTS is provided by this PIA, the associated Trade Transparency Analysis and Research (TTAR) System of Records Notice (SORN) (74 FR 39083) and Final Rule (74 FR 38887) published in the *Federal Register*.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1. What information is collected, used, disseminated, or maintained in the system?

DARTTS routinely receives bulk financial and trade information collected by other agencies and foreign governments, hereafter referred to as "raw data." The agencies that provide DARTTS with trade data collect PII directly from individuals or enterprises that are required to complete import-export forms. The agencies that provide DARTTS with financial data receive PII from individuals and institutions, such as banks, that are required to complete certain financial reporting forms. This raw data contains the following PII, listed by category of information (see Table 1 below):

Table 1. Personally Identifiable Information in DARTTS

Category of Information	Personally Identifiable Information
U.S. Trade Data	Names and Addresses (home or business) of importers, exporters, brokers, consignees and shippers Importer IDs Exporter IDs Broker IDs Manufacturer IDs
Foreign Trade Data[3]	Names of importers, exporters, and brokers Addresses of importers and exporters Importer IDs Exporter IDs Broker IDs Manufacturer IDs
U.S. Financial Data	Names of individuals engaging in financial transactions that are reportable under the Bank Secrecy Act (*e.g.*, cash transactions over $10,000) (See 1.2, ¶ 5.)

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

	Addresses Date of Birth Social Security/Taxpayer Identification Numbers Passport Number and Country of Issuance Bank Account Numbers Party Names and Addresses (i.e., person who made the transaction) Owner Names and Addresses (i.e., person on whose behalf the transaction is made)

In some instances, the Importer ID and Exporter ID is the individual or entity's Social Security or Tax Identification Number. Importers and exporters may be individuals (US Citizens, Lawful Permanent Residents, and aliens), corporations, or other business entities.

DARTTS also uses analytical tools to create user-driven analyses of the raw data. These analyses can 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 vary depending upon the analytical tool selected and parameters set by the user. The analyses may include, for example, high-level graphical representations that reveal trade pricing discrepancies or itemized listings of specific transactions identified during analysis as potentially indicative of fraud or other illegal activity.

DARTTS also creates extracts of U.S. trade data that have been stripped of PII, and provides those extracts to partner countries that operate their own trade transparency programs and with whom the United States has entered into a Customs Mutual Assistance Agreement or other similar information sharing agreement. DARTTS strips all PII from the U.S. trade data and assigns a random identification number in place of all importer ID numbers. DARTTS creates a table that allows users to trace back to the original DARTTS data by using the random identification number. The table is used by ICE to respond to inquiries from foreign government TTUs if they identify suspicious U.S. trade transactions of interest to the foreign customs officials. The information collected by CBP on the FinCEN 105, Report of International Transportation of Currency or Monetary Instruments (CMIR), may be shared on a case by case basis under the authority of existing Customs Mutual Assistance Agreements. The other U.S. financial data described above is not shared with the partner countries.

1.2. What are the sources of the information in the system?

All of the raw data in DARTTS is provided by other U.S. agencies and foreign governments. ICE does not directly collect information from individuals or entities for inclusion in DARTTS. The raw data within DARTTS is divided into three broad categories: U.S. trade data, foreign trade data, and U.S. financial data. The specific sources of the raw data are:

(1) U.S. Customs and Border Protection (CBP) import data. CBP collects this data from individuals and entities who import merchandise into the U.S. and complete CBP Form 7501, Entry Summary and/or provide electronic cargo inventory and carrier manifest information via the Automated Manifest System (AMS). CBP provides this data to ICE in the form of an extract

from CBP's Automated Commercial System (ACS), which will eventually be transitioned to CBP's Automated Commercial Environment (ACE).

(2) U.S. Customs and Border Protection (CBP)/U.S. Department of Commerce, Census Bureau export data. This data is collected electronically via the Automated Export System (AES), a system jointly operated by CBP and U.S. Census Bureau. As of September 2008, all exporters are required to file electronic export information through AES.

(3) U.S. Department of Commerce export data. Historically, Commerce collected this data from individuals and entities who exported commodities from the U.S. using Commerce Department Form 7525-V, "Shipper's Export Declaration," prior to September 2008. In June of 2008, Commerce published a final rule in the Federal Register (73 FR 31548) mandating electronic filing of export information via AES beginning in September 2008.

(4) U.S. Exports of Merchandise Dataset. This is publicly available aggregated U.S. export data purchased from the U.S. Department of Commerce. This dataset does not contain any PII. The dataset is further described (including a complete list of the data fields) and can be purchased through the following Commerce Department website:

http://www.census.gov/foreign-trade/reference/products/catalog/expDVD.html

(5) Foreign import and export data. This data is provided to ICE by partner countries pursuant to a Customs Mutual Assistance Agreement 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 individuals' names and other identifying information that may be contained in trade records.

(6) Financial Transaction Reports from the Treasury Department's Financial Crimes Enforcement Network (FinCEN). FinCEN administers the Bank Secrecy Act (BSA)[4], a comprehensive Federal anti-money laundering statute. The BSA requires depository institutions and other industries vulnerable to money laundering to take precautions against financial crime, including reporting financial transactions possibly indicative of money laundering. FinCEN provides DARTTS with the following reporting data:

- Report of International Transportation of Currency or Monetary Instruments (CMIRs)—Declarations of currency or monetary instruments in excess of $10,000 made by persons coming into or leaving the United States.
- Currency Transaction Reports (CTRs)—Deposits or withdrawals of $10,000 or more in currency into or out of depository institutions, casinos and card clubs.
- Suspicious Activity Reports (SARs)—Information regarding suspicious financial transactions within depository institutions, the money services business industry, the securities and futures industry, casinos and card clubs.

[4] Pub. L. 91-508, titles I, II, October 26, 1970, 84 Stat. 1114, 1118 (31 U.S.C. § 1051 et seq).

- Form 8300 - Report of Cash Payments over $10,000 Received in a Trade or Business—Reports of merchandise purchased with $10,000 or more in currency.
- Foreign Bank Account Report (FBAR) – Report of financial interest in foreign financial account in excess of $10,000.

Additionally, DARTTS itself is the source of analyses of the raw data produced using analytical tools within the system and the extracts of U.S. trade data that are provided to foreign partners.

1.3. Why is the information being collected, used, disseminated, or maintained?

DARTTS uses the trade and financial information collected by other governmental entities to aid ICE investigations of criminal violations of U.S. laws. The raw data loaded into DARTTS allows analysts to compare the information from different import-export and financial transactions to identify anomalies or other suspicious patterns or activities. The PII in the raw data is necessary because it is used to link related transactions together. It is also necessary to identify the persons or entities that should be investigated further.

Table 2 lists the sources of specific PII in DARTTS and reasons the PII is needed.

Table 2. Personally Identifiable Information in DARTTS

Sources of U.S. Information	Personally Identifiable Information	Reason Needed
U.S. Trade Data and Foreign Trade Data		
	Names	Used to identify individuals 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.
	Addresses	
	Trade ID Numbers (e.g., Importer ID)	
U.S. Financial Data		
	Names	Used to identify individuals 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.
	Addresses	

Sources of U.S. Information	Personally Identifiable Information	Reason Needed
	Social Security Numbers (SSNs) Tax Identification Number Trade ID Numbers (e.g., Importer ID)	Used as unique identifier of an individual. For example, analysts can use a SSN as one of the parameters in a search to potentially find SSNs that are associated with more than one individual. 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 numbers	Used in a similar way as SSNs, passport numbers are generally unique and are used to identify individuals.
	Bank account numbers	Used to identify the bank or depository institution and the individual involved in the transaction. Used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects.

1.4. How is the information collected?

As stated earlier, ICE does not directly collect information from individuals or entities for inclusion in DARTTS. Instead, ICE receives the raw data from the sources listed in Question 1.2 via CD-ROM, web download, or external storage devices and loads the data into DARTTS. DARTTS does not receive any data via direct electronic transmission from another system.

The U.S. Government agencies listed in Section 1.2 collect the trade and financial data from individuals and enterprises using various forms. The forms are listed in Table 3 below, including the OMB Control Number for each form issued pursuant to the Paperwork Reduction Act.

Table 3. 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
	Commerce Department Form 7525-V, "Shipper's Export Declaration," OMB Control No. 0607-0152 (prior to September 2008)
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
	Treasury Form TD-F- 90-22.47, "Suspicious Activity Report by Depository Institutions," OMB Control No. 1506-0001
	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 90-22.1, "Report of Foreign Bank and Financial Accounts," OMB Control No. 1545-2038

1.5. How will the information be checked for accuracy?

All of the information in DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority. The original data collector is responsible for maintaining and

checking the accuracy of its own data and has various means to do so. The majority of the data loaded into DARTTS is highly accurate because data has been collected directly from the individual or entity. In other instances, however, the data about individuals or entities is provided to the governmental organization by a third party.

DARTTS cannot independently verify the accuracy of the data it receives. FinCEN currently provides ICE with corrections to U.S. Financial Data, which are then uploaded to DARTTS. ICE does not receive corrections from its sources of trade data. In the event that errors are discovered, the DARTTS system owner will notify the originating agency.

Additionally, DARTTS data is never used directly as evidence to prosecute crimes. DARTTS is solely an analytical tool that helps investigators identify anomalies and suspicious activity in large sets of data. It is important to note that not all anomalies are indicators of criminal activity. It is incumbent upon the investigator that finds the anomaly to fully check all original data sources and to 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. When investigating potential violations of U.S. laws, ICE investigators are required to obtain and verify the original source data from the original data collector to prevent inaccurate information from propagating.

1.6. What specific legal authorities, arrangements, and/or agreements authorized the collection of information?

ICE has been authorized to collect information under 18 U.S.C. § 545 (Smuggling goods into the United States); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); and 19 U.S.C § 1484 (Entry of Merchandise).

1.7. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

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 or append the data, which eliminates the potential for user-generated data errors. Additionally, ICE agents and investigators will fully investigate leads generated by 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 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 when disparate data are aggregated because the use of the aggregated data is inconsistent with the purpose for which the data was originally collected.

Mitigation: This risk is mitigated by limiting usage of 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 2.0 Uses of the information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all uses of the information.

ICE uses the information in DARTTS to conduct analyses of raw financial and trade data to identify potential violations of U.S. 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. DARTTS conducts three types of analyses:

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

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

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

ICE TTU investigators with experience conducting financial, money laundering, and trade fraud investigations use the completed analysis to identify possible criminal activity and provide support to field investigators. TTU investigators at ICE Headquarters refer the results of DARTTS analyses to ICE 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 ICE investigators. ICE investigators in the domestic field offices can also independently generate leads and subsequent investigations using DARTTS analysis. In addition, ICE investigators in attaché offices at U.S. embassies abroad have access to DARTTS on stand-alone terminals. These investigators use DARTTS to conduct analyses in support of financial, money laundering, and trade fraud investigations, and to respond to inquires from partner-country TTUs with whom ICE shares anonymized U.S. trade data.

DARTTS-created extracts of U.S. trade data, excluding financial data, are provided to partner countries that operate their own trade transparency programs and with whom the United States has

entered into a Customs Mutual Assistance Agreement or other similar information sharing agreements. This data is shared with these foreign countries' own TTUs and is used to conduct similar analyses as those described in this PIA. ICE representatives at the U.S. embassies will respond to inquiries from foreign TTUs that have identified suspicious U.S. trade transactions of interest. Once ICE has validated that these transactions are suspicious, ICE will share additional information from those specific trade records, including information that identifies persons or entities, with the foreign TTU to further their investigations, in accordance with CMAA and other similar information sharing agreements. ICE may also open its own investigation into the matter.

2.2 What types of tools are used to analyze data and what type of data may be produced?

DARTTS uses the commercial software program LEADMiner to analyze raw trade and financial data to identify anomalies and other suspicious transactions. These anomalies can be indicators of trade-based money laundering or other import-export crimes.

LEADMiner is an application designed for experienced investigators. It enables the analysis of structured and unstructured data by using three tools: the drill-down technique; link analysis; and charting and graphing tools that use proprietary statistical algorithms. LEADMiner allows non-technical users with investigative experience to analyze large quantities of data and rapidly identify problem areas. The program makes it easier for investigators to apply their specific knowledge and expertise to ever-larger sets of data.

Investigators can use the drill-down system to quickly find, analyze, share, and document suspicious patterns in large amounts of data. The drill-down system allows investigators to continually observe and analyze patterns in data at any point as they progress toward the targeting goal. As they drill down and focus on specific parts of the data, the system may identify patterns or anomalies that the investigators recognize as suspicious. This tool provides investigators an easy way to continue to drill down or up through the data to search for a similar pattern elsewhere without losing track of where they are. Investigators can also search multiple datasets for the same suspicious people, entities, or patterns.

In response to user-specified queries, DARTTS can also conduct "link analysis," which identifies links (relationships) 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 may help investigators identify potentially criminal activity, suspicious transactions, witnesses, or suspects. DARTTS also provides investigators the means to represent data graphically in graphs, charts, or tables to make visual identification of anomalous transactions easier.

The various tools available through LEADMiner allow investigators to produce analytical results on their screens by using the capabilities described above. These results provide different ways of looking at the original data. Investigators can also save results, in electronic format, which is readable by other analysis tools outside of DARTTS. This facilitates further analysis and allows the investigator to print out results for reference or retention in a case file. DARTTS does not perform entity resolution nor does it create new records in DARTTS.

2.3 If the system uses commercial or publicly available data, please explain why and how it is used.

As described in question 1.2 above, ICE purchases from the U.S. Department of Commerce a publicly available dataset called the U.S. Exports of Merchandise. This dataset contains aggregate U.S. export data but does not contain any PII. This information facilitates international trade discrepancy analysis by allowing ICE to compare U.S. exports to import data provided by partner countries. Analyzed information typically focuses on a particular commodity and includes the value, quantity, method of transportation, and shipping weights of exported merchandise. Without this U.S. export data, international trade discrepancy analysis is not possible.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Privacy Risk: There is a risk that PII will be accessed by unauthorized individuals or for unauthorized purposes.

Mitigation: This is mitigated by limiting DARTTS access to ICE investigators who use it to conduct official criminal investigative activities. As described in Section 8 of this document, security and access controls are in place to mitigate the risk of unauthorized individuals gaining access to PII. Users take mandatory annual privacy and security training, which stresses the importance of authorized use of personal data in government systems. Individuals who are found to access or use the DARTTS data in an unauthorized manner will be disciplined in accordance with ICE policy. 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 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 investigators will fully investigate leads generated by 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 the investigator has no need to further investigate for criminal violations. Any and all information obtained from DARTTS will be independently verified before it is acted upon or included in an ICE investigative or analytical report.

Finally, ICE shares U.S. trade information with its partner country customs agencies in an anonymized form to reduce the unnecessary sharing of personal data. ICE will only share personal information with the foreign customs officials once a suspicious transaction has been identified. This greatly limits the sharing of personal data to only those situations in which a law enforcement investigation will be initiated by a foreign or domestic law enforcement agency.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

All data stored in DARTTS is retained. This data includes everything noted in Question 1.2 as well as reports generated by DARTTS users and audit logs of user activity. Additionally, ICE retains the original CD-ROMs, external storage devices and electronic data transfers that contain the raw data uploaded into DARTTS. All external media is maintained in a secure location in the TTU offices at ICE Headquarters until the end of the retention period, at which time the data is destroyed per ICE policy.

3.2 How long is information retained?

In November 2009, the National Archives and Records Administration (NARA) approved a record retention schedule for the information maintained in DARTTS. ICE maintains the records in DARTTS for five (5) years and then archives the records for five (5) additional years, for a total retention period of ten (10) years. The five-year retention period for records is necessary to create a data set large enough to effectively identify anomalies and patterns of behavior in trade transactions. Records older than five (5) years will be removed from the system and archived for five (5) additional years and will only be used to provide a historical basis for anomalies in current trade activity. The original CD-ROMs, external storage devices or electronic data transfers containing the raw data will be retained for five (5) years to ensure data integrity and for system maintenance.

3.3 Has the retention schedule been approved by component records officer and the National Archives and Records Administration (NARA)?

Yes. In November 2009, the ICE Records Management Branch and NARA approved a record retention schedule (as described in Question 3.2) for the information maintained in DARTTS.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The ten (10) year retention period proposed for DARTTS 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 more than ten (10) years old to conduct the types of analyses described in this

document. The ten (10) year retention for the DARTTS database ensures that sufficient information is available to conduct meaningful analyses for law enforcement purposes, while not keeping the information any longer than necessary.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared, and for what purpose?

DARTTS analytical results are shared within DHS for law enforcement investigatory purposes on a case-by-case basis. ICE may share this information with other parts of DHS, but only after the underlying data has been validated and only for law enforcement or homeland security purposes. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

4.2 How is the information transmitted or disclosed?

DARTTS analytical results are not routinely disclosed to other parts of DHS. Disclosures are made on a case-by-case basis and transmission or disclosure methods will vary depending on the circumstances. Because this data is law enforcement sensitive and may contain PII, appropriate safeguards (e.g., encrypted media) are used to ensure the security of the data during transmission or disclosure.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: There is a risk of unauthorized or improper dissemination of data contained in DARTTS.

Mitigation: DARTTS analytical results are shared within DHS only for law enforcement or homeland security purposes, and only on a case-by-case basis. The ICE agent in charge of an investigation determines whether to share this information based on the needs and direction of that investigation. Data is only shared once it is validated. This ensures that ICE experts are the gatekeepers for appropriate analysis of financial and trade data within DARTTS. When disclosures are deemed necessary or helpful to an investigation, appropriate steps are taken to secure the information.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, State, Local and Tribal government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

DARTTS analytical results may be shared outside of DHS for law enforcement investigatory purposes on a case-by-case basis with other Federal, State, local and foreign agencies. ICE only shares this information after the underlying data has been validated and only for law enforcement or homeland security purposes. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

In addition, DARTTS-created extracts of U.S. trade data are provided to partner countries that operate their own trade transparency programs and with whom the United States has entered into a Customs Mutual Assistance Agreement or other similar information sharing agreement. This data is shared in an anonymized form with these foreign countries' own TTUs and are used to conduct similar analyses as those described in this PIA. ICE representatives at the U.S. embassies will respond to inquiries from foreign TTUs that have identified suspicious U.S. trade transactions. Once ICE has validated that the transactions are suspicious, ICE will share identifiable information from those trade records with the foreign TTU to further their customs investigations. ICE may also open its own investigation into the matter.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The Trade Transparency Analysis and Research (TTAR) SORN (DHS/ICE-005, August 5, 2009 74 FR 39083) applies to DARTTS information and includes routine uses to 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 Customs Mutual Assistance Agreements or other similar agreements to further the identification and prosecution of trade-based money laundering, contraband smuggling, and trade fraud. This external sharing is compatible with the law enforcement purpose of DARTTS and is necessary for

the proper administration of a government program. The TTAR SORN and Final Rule were published in the *Federal Register*, on August 5, 2009.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

DARTTS analytical results are not routinely disclosed outside of DHS. Disclosures are made on a case-by-case basis and transmission or disclosure methods will vary depending upon the circumstances. Because this data is law enforcement sensitive and may contain PII, appropriate safeguards (e.g., encrypted media) are used to ensure the security of the data during transmission or disclosure. Additionally, the recipient of DARTTS analytical data is typically another law enforcement agency which has proper procedures and training in place to safeguard investigatory data. Prior to any information being shared, the recipients would be required by ICE to safeguard the information in accordance with its sensitivity.

The anonymized U.S. trade data is shared in bulk with partner countries through the secure transfer of encrypted media, through an ICE representative (who is usually an ICE agent or investigator) If an investigation is initiated, and personal information is shared with the foreign TTU, the ICE representative will provide only pertinent information, either verbally or in writing. The ICE representative will also note the exchange of information in a report of investigation or other documentation. In addition, foreign governments secure the U.S. trade information pursuant to the terms of information sharing agreements, which include provisions for the physical and logical protection of sensitive information. All foreign TTUs are located within official government offices and are secured in accordance with each foreign government's physical and technical security requirements.

5.4 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Privacy Risk: There is a privacy risk of unauthorized or improper dissemination of data contained in DARTTS.

Mitigation: ICE routinely shares anonymized U.S. trade data with foreign partners pursuant to international agreements. The data is not shared in identifiable form to limit the dissemination of personal information to only that which is necessary to further a law enforcement interest or investigation based on a suspicious transaction. Identifiable information from U.S. trade data is only shared with foreign customs agencies by ICE on an ad hoc basis if the partner has identified a suspicious transaction and then only for the purpose of permitting the foreign customs agency to investigate whether a violation of law has occurred.

DARTTS analytical results are shared outside of DHS only for law enforcement or homeland security purposes, and only on a case-by-case basis. The ICE agent in charge of an investigation determines whether to share DARTTS data based on the needs and direction of that investigation. Data is only shared once it is validated. When disclosures are deemed necessary or helpful to an investigation,

appropriate steps are taken to secure the information during transmission. Recipients of DARTTS results are typically other law enforcement agencies that have proper procedures and training in place to properly safeguard investigatory information. In addition, all external sharing will comply with ICE and DHS policies.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

ICE does not directly collect information from individuals or entities for use in 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 (SORNs). The following SORNs are published in the *Federal Register* and describe the raw data ICE receives from U.S. agencies for use in DARTTS (Table 4 below):

Table 4. Privacy Act System of Records Notices

Agencies	Systems of Records Notices
FinCEN Information	Suspicious Activity Report System (Treasury/FinCEN .002, August 8, 2005, 70 FR 45756) Bank Secrecy Act Reports System (Treasury/FinCEN .003, August 8, 2005, 70 FR 45756)
Commerce Department Information	Individuals Identified in Export Transactions System (Commerce/ITA-1)
CBP Information	Automated Commercial System (DHS/CBP-015, December 19, 2008 73 FR 77759) Automated Commercial Environment/International Trade Data System (ACE/ITDS) (DHS/CBP-001, January 19, 2006, 71 FR 3109)

Notice of the existence and operation of DARTTS is provided by this PIA, and the TTAR SORN and Final Rule published in the *Federal Register*.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

All information provided to DARTTS by U.S. agencies is required by U.S. law to be provided to the agencies that originally collected the information. Individuals and corporations may choose to not import or export goods, for example, but should they choose to undertake such trade activities, the information is required by the collecting agencies.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

ICE is not aware that the U.S. agencies that collect this information provide individuals and entities any right to consent to the particular uses of the information. However, all information is collected for the purpose of regulating trade and enforcing U.S. import-export and financial criminal laws. ICE's use of the information it receives is consistent with the purpose of the collection.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: There is a risk that individuals may not be aware their information may be contained within DARTTS.

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

Because 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 7.0 Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals may request access to records about them in DARTTS by following the procedures outlined in the DARTTS SORN. 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 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.

In addition to the procedures above, 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 FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If individuals obtain access to the information in DARTTS pursuant to the procedures outlined in the DARTTS SORN, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the DARTTS SORN. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

In addition to the procedures above, 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 FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in the TTAR SORN and in this PIA in Questions 7.1 and 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

It is the primary responsibility of the original source data owners to maintain accurate information and provide a means for individuals to access and correct inaccurate records. As stated, individuals may submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis. Individuals also may have the opportunity to contact the Federal agency that originally collected the information about them using the procedures described in those agencies' SORN.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Redress is available through requests made under the Privacy Act as described above; however, providing individual access and/or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in 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. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

It is important to note that DARTTS data is never used directly as evidence to prosecute crimes. DARTTS is solely an analytical tool which helps in the identification of anomalies and not all anomalies are indicators of criminal activity. It is incumbent upon the investigator who finds the anomaly to fully check all original data sources and further investigate to the reason for the anomaly. If the anomaly can be legitimately explained, the investigator has no need to further investigate the anomaly for criminal violations. As a safeguard, when investigating potential violations of U.S. laws, ICE investigators are required to obtain and verify the original source data from the agency that collected the information to prevent inaccurate information from propagating.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Access to DARTTS is limited to ICE users with an established need-to-know to perform their prescribed duties. User access roles are approved by a supervisor and implemented by the DARTTS Administrator. Currently DARTTS has three user roles:

- DARTTS User – Investigate financial or trade transactions, conduct analysis, and generate reports

- DARTTS Supervisor – Investigate financial or trade transactions, conduct analysis, generate reports, assign user roles, and perform user and activity auditing
- DARTTS Administrator – Create, activate, revoke and/or remove user access and accounts

DARTTS users are authenticated using the ICE Enterprise Network single-sign-on validation process. DARTTS access is granted on a case-by-case basis by the DARTTS Administrator, who is designated by the TTU Unit Chief. User access roles are reviewed regularly by a supervisor to ensure that users have the appropriate access and that users who no longer require access are removed from the access list. Additionally, access to DARTTS is limited to ICE Special Agents and Criminal Research Specialists who work on TTU investigations at Headquarters or in the ICE field and foreign attaché offices, as well as properly cleared support personnel. This access is further limited only to individuals who have access to the ICE enterprise network and foreign attaché offices that have stand-alone DARTTS terminals. Access is strictly limited to individuals who are directly involved in supporting the mission of the ICE TTU.

8.2 Will Department contractors have access to the system?

Yes. Certain contractors who are cleared through ICE personnel security have access as necessary to complete information technology development and operations and maintenance tasks on the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

DARTTS users receive system-specific training that emphasizes the use limitations and other safeguards discussed in this PIA. In addition, all ICE personnel and contractors complete annual mandatory privacy and security trainings, the Culture of Privacy Awareness and the Information Assurance Awareness Training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The DARTTS Enterprise and stand-alone systems are undergoing a Certification and Accreditation process, which is expected to be complete in April 2010.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

User authentication is restricted to valid ICE users and follows the ICE single sign on validation process. Access roles are approved by a supervisor and implemented by the DARTTS Administrator. Access roles are reviewed regularly to ensure that users have the appropriate access. Individuals who no

longer require access are removed from the access list. Access is audited and the audit logs are reviewed on a regular basis.

DARTTS employs enhanced auditing capabilities that allow for both real time monitoring and the generation of audit logs, which are used to track user activities and provide accountability. Only authorized personnel can access audit trails, which are kept for a minimum of 90 days. Audit trails are reviewed on a weekly basis by DARTTS Administrators or the Information System Security Officer (ISSO). The system administrator also maintains a spreadsheet record of the receipt or distribution of sensitive information on electronic media.

Trade data received from CBP is transferred to ICE via secure encrypted media. FinCEN and Department of Commerce information is received via secure electronic data transmission (i.e., web download). All external media is maintained in a secure location in the TTU offices at ICE Headquarters until the end of the retention period, at which time the data is destroyed per ICE policy.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: The risks are unauthorized access to or misuse of data contained within DARTTS.

Mitigation: This is mitigated by the security training users complete that explains how to protect sensitive information, and by the use of audit mechanisms that log and monitor user activity. These risks have been further mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include user access controls, auditing, intrusion detection software, and user training. Trained, cleared analysts each have individual accounts for accessing DARTTS and system usage is audited on a regular basis.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

DARTTS is an IT system with data analysis tools supporting the identification of anomalies or patterns of conduct that may indicate criminal activity.

9.2 What stage of development is the system in and what project development life cycle was used?

DARTTS is in the Operations and Maintenance stage of the ICE System Development Life Cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

Systems like DARTTS that analyze data and produce results seeking to identify suspicious transactions for further investigation present the risk that the model being used to identify leads is not valid. An invalid model may identify individuals or entities as suspects who are not actually engaged in illegal activities, possibly subjecting them to unwarranted government attention and investigation.

In the case of DARTTS, this risk is mitigated by the fact that DARTTS does not seek to predict future behavior or "profile" individuals, *i.e.*, it does not look for individuals who meet a certain pattern of behavior that has been pre-determined to be suspect. Instead, it analyzes trade and financial transactions and identifies those that are statistically anomalous. Investigators follow up on anomalous transactions to determine if they are in fact suspicious and warrant further investigation. Investigators gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination. Not all anomalies lead to formal investigations, and not all investigations are centered on individuals.

DARTTS can also identify links (relationships) 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 sometimes help investigators to identify potentially criminal activity and lead to identification of other suspicious transactions, witnesses, or other suspects.

Responsible Official

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

Approval Signature Page

Original copy signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security