Privacy Impact Assessment Update for the

Data Analysis & Research for Trade Transparency System (DARTTS)

DHS/ICE/PIA-006(b)

April 2, 2012

Contact Point
James A. Dinkins
Executive Associate Director
Homeland Security 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

U.S. Immigration and Customs Enforcement (ICE), a component agency within the Department of Homeland Security (DHS), 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, and re-published with changes in April 2010. With this update to the PIA, ICE is adding two new data sets to DARTTS and modifying its retention period. ICE is also expanding the use of DARTTS within DHS to permit select U.S. Customs and Border Protection (CBP) customs officers and import specialists to access and use the system. Finally, ICE is establishing a separate instance of DARTTS for use by foreign government partners that operate trade transparency units and have customs information sharing agreements with the United States. This new "Foreign DARTTS" system is maintained in a secure, web-based environment hosted by ICE. Foreign DARTTS permits authorized foreign partners to use the DARTTS tools to analyze a more limited set of DARTTS data in support of their own trade-based investigations.

Introduction

DARTTS is owned and operated by the ICE Homeland Security Investigations (HSI) Trade Transparency Unit (TTU). Trade transparency is the concept of examining U.S. and foreign trade data to identify anomalies in trade transactions that may indicate trade-based money laundering or other import-export crimes that ICE is responsible for investigating. ICE uses DARTTS to conduct trade transparency analysis in order to identify and investigate these illegal activities. As part of the investigative process, HSI agents 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 identification of anomalies for the investigator.

DARTTS allows ICE to perform research and analyses not possible in any other ICE system because of the data it contains and the levels of detail at which the data can be analyzed. For instance, DARTTS allows agents and analysts 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. Agents then analyze such 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 deciding whether to investigate further.

Updates to the DARTTS System

ICE is making several changes to DARTTS. First, ICE is adding two law enforcement data sets to DARTTS: TECS subject records and the Specially Designated Nationals (SDN) List.[1] The addition of this law enforcement data enhances the analytical capabilities of the system and improves ICE's ability to identify suspicious trade and financial transactions. The TECS subject records include Person Subject, Vehicle Subject, Vessel Subject, Aircraft Subject, Thing Subject, Business Subject, and Organization Subject Records.[2] 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 also contain PII that is related to the subject record, such as a Vehicle Subject Record that may contain the vehicle owner's name. DARTTS only uses subject records created by ICE or CBP, and not by other law enforcement agencies. Including ICE and CBP subject records in DARTTS allows users to quickly determine when an entity being researched in DARTTS is already part of a pending HSI investigation or was involved in an investigation that is now closed.

The SDN List is an economic and trade sanctions program based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, and other threats to the national security, foreign policy or economy of the United States. Including the SDN List in DARTTS allows HSI users to quickly identify international trade and/or financial transactions that are associated with a specially-

[1] Concurrent with the publication of this PIA update, ICE is modifying the DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) System of Records Notice (SORN) to describe the new data sets that are maintained in this system.

[2] The PIA for DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, December 23, 2010, is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf. The DHS/CBP-011 TECS SORN was last published December 19, 2008 (73 Fed. Reg. 77778).

designated individual or entity, which allows HSI to take appropriate investigative actions in a timely and more efficient manner.

Second, ICE intends to modify the retention period to retain DARTTS data in the system for ten years. The current retention policy retains data in DARTTS for five years, and then in an archive for another five years. ICE is lengthening the retention of data in the system to better support information exchanges with foreign partners who use Foreign DARTTS and to improve the identification of anomalous transactions in the DARTTS system by analyzing data over a longer period of time.

Third, ICE is authorizing CBP customs officers and import specialists to access and use DARTTS to conduct trade transparency analysis. These CBP employees use DARTTS in support of the CBP mission to enforce U.S. trade laws and ensure the collection of all lawfully owed revenue from trade activities. Like HSI agents and analysts at ICE that use the system, CBP customs officers and import specialists will use DARTTS to identify anomalous transactions that may indicate violations of U.S. trade laws. If HSI elects not to open an investigation into these transactions, CBP may initiate administrative enforcement actions to recover delinquent revenue or penalties. CBP's use of DARTTS will help DHS more efficiently enforce U.S. trade laws. Not all suspicious or anomalous transactions identified in DARTTS will lead to DHS investigations or enforcement actions.

Fourth, ICE is modifying the DARTTS system to permit authorized users to access it from mobile devices. This will permit HSI and CBP users to conduct trade transparency analysis using government-furnished tablet computers and other mobile devices. This change allows DARTTS to be used in real-time enforcement encounters where accessing the system through a laptop or desktop government computer may be impractical or inefficient. ICE is employing robust security controls to ensure that use of DARTTS on a mobile platform does not compromise the security protections of the system or its data.

Finally, ICE is launching a separate web-based instance of the DARTTS system called "Foreign DARTTS" that is specifically dedicated to the use of foreign government partners that operate trade transparency units and have signed customs mutual assistance agreements (or similar information sharing agreements) with the United States. Foreign DARTTS will replace the current method by which these partners use DARTTS, which involves stand-alone computers located in the foreign partner's office that is loaded with anonymized U.S. trade data as well as the foreign partner's own trade data. ICE has supported the operation of these stand-alone DARTTS terminals by traveling to the foreign partner's office to update software and load new data into the system. To reduce costs and improve security, Foreign DARTTS was created to provide an Internet-based version of DARTTS hosted on the ICE network. In Foreign DARTTS, each foreign partner accesses only the data it is authorized to see as a result of user roles established in the system and managed by ICE. With Foreign DARTTS, there is no change in the data these foreign users can access or in the analytical tools available for their use.

Although it contains the same software, Foreign DARTTS is a completely separate system from DARTTS and does not contain the same data. Foreign DARTTS only contains trade data provided by the foreign partners that use the system, and anonymized U.S. trade data that contains trade transactions between the United States and those foreign partners. Foreign DARTTS does not contain the U.S. financial transaction data or law enforcement data that is maintained in DARTTS. Foreign DARTTS relies on user roles to ensure that access privileges are enforced according to the information sharing agreements in place among the parties. Unless the countries have agreed to broader information sharing arrangements, the system will only permit foreign users to view their own nation's trade data and anonymized U.S. trade transactions between their nation and the United States. Foreign trade data is loaded into Foreign DARTTS after the foreign partner uploads the raw data to a secure FTP server at ICE. ICE formats the data and loads it into Foreign DARTTS and tags it so the system will be able to apply the appropriate user access rules to the data.

Reason for the PIA Update

The original DARTTS PIA was published on October 2008 and then re-published in April 2010. Since the most recent update, user needs have changed and new data requirements have been identified. With this PIA update, ICE is notifying the public of several changes to the DARTTS system that expand the type of data used by the system, lengthen the time that data is retained in the system, and authorize certain CBP personnel to use the system to conduct trade transparency analysis. This update also describes the support of mobile device access to DARTTS and the creation of Foreign DARTTS for use by foreign government partners who are also engaging in trade transparency efforts and cooperatively sharing information with the United States.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

With this update, ICE is notifying the public of the addition of two law enforcement data sets to DARTTS: TECS subject records and the SDN List. The addition of this law enforcement data enhances the analytical capabilities of the system and improves ICE's ability to identify suspicious trade and financial transactions. Concurrent with the publication of this PIA update, ICE is modifying the DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) System of Records Notice (SORN) to describe the new data sets that are maintained in this system.

The subject records added to DARTTS were created by ICE and CBP personnel in the CBP database known as TECS (CBP/PIA-009(a) TECS System). Subject records contain information on persons, vehicles, vessels, businesses, aircraft, and ‘things’ that are related to a law enforcement investigation or other matters. DARTTS only uses subject records created by ICE or CBP, and not by other law enforcement agencies. Individuals described in Person Subject Records may be individuals who are or were targets of law enforcement investigations or actions by ICE or CBP, but can also include witness information. Person Subject Records can also include individuals who are not targets in any law enforcement action by ICE or CBP but are seeking approval for a license, such as applicants for Customs brokers licenses, or to operate a Customs-bonded warehouse, or be a bonded carrier, or bonded cartman. Victim data in Person Subject Records is not imported into DARTTS. Including these subject records in DARTTS allows users of the system to quickly determine if an entity that is being researched in DARTTS is already related to a pending or closed DHS investigation or other DHS law enforcement action. Before this data was included in DARTTS, HSI investigators would run manual queries in TECS to determine if an investigative link existed. The inclusion of these records in DARTTS improves the efficiency HSI investigations and CBP’s ability to enforce trade laws and collect lawfully owed revenues.

TECS subject records includes some or all of the following PII data: individual name, address, date of birth, Social Security Number/Taxpayer Identification Number (SSN/TIN), passport number, country of issuance, bank account number(s), telephone number(s), driver’s license number and state of issuance, alien registration number (A-Number), business name, vehicle license plate, vehicle description, vessel names, vessel description, aircraft name, aircraft tail number, aircraft description. CBP provides routine data extracts of TECS subject records to ICE via a secure FTP site, after which ICE ingests the subject records into DARTTS.

The SDN List is an economic and trade sanctions program based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, and other threats to the national security, foreign policy or economy of the United States. Collectively, such individuals and entities are called “Specially Designated Nationals.” The inclusion of the SDN List in DARTTS allows HSI users to quickly and efficiently identify international trade and/or financial transactions that are conducted with a Specially Designated National and to focus investigative resources on such transactions as appropriate. The SDN list is compiled by the U.S. Department of the Treasury’s Office of Foreign Asset Control (OFAC), and is made publicly available on the OFAC website.

The SDN List contains the names of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. By law, their U.S. assets are blocked and U.S. persons are generally prohibited from dealing with them. The SDN List contains some or all of the following PII: individual name, business name, address, date of birth, SSN/TIN, and passport number. ICE downloads this list (which is publicly available) from the OFAC website, and uploads it into DARTTS.

The incorporation of these law enforcement data sets in DARTTS creates new privacy risks. Specifically, if this data is out of date, inaccurate, incomplete or otherwise misleading, it could result in investigative activities that are unwarranted. This risk is mitigated by the frequency with which TECS and SDN List information is updated in DARTTS, specifically TECS data will be updated quarterly and the SDN List will be updated monthly. Furthermore, before completing their analytical report and or taking further action, DARTTS users are required to cross check their analytical products from DARTTS against the actual source records, to include running queries in TECS and pulling the most updated SDN List from the Treasury website. Also, as part of normal investigative protocol, HSI agents and analysts conduct additional research outside of DARTTS to determine why an individual's name was in TECS or on the SDN List before relying on this information to make important decisions during an investigation. This would likely reveal any problems with the data at an early stage and minimize the risk of DHS relying on this information in error. This risk is further mitigated by the fact that DARTTS does not allow users to modify or append the data, which eliminates the potential for user-generated data errors. For individuals on the SDN List, because it is public, individuals are typically aware of their inclusion on the List and may petition the U.S. Department of the Treasury to have their name removed. The public nature of the List and the availability of redress to affected individuals also mitigates the risk that the SDN List data is inaccurate.

Uses of the System and the Information

ICE is expanding the use of DARTTS by granting select CBP officers and import specialists direct user access to DARTTS. These employees conduct trade transparency analysis in DARTTS in furtherance of CBP's mission to enforce U.S. trade laws and ensure the collection of all lawfully owed revenue from trade activities. This change expands the use of DARTTS to include the civil enforcement of U.S. trade laws. Because the scope of CBP's authorities is not as broad as HSI, CBP employees are assigned more restricted user roles in the system. Specifically, CBP users are only authorized to access trade and law enforcement data, but not financial transaction data, in DARTTS.[3]

CBP employees use DARTTS to identify anomalous trade transactions that may indicate violations of U.S. trade laws. HSI will first determine whether to open an investigation into suspicious transactions. If HSI declines, CBP may take administrative enforcement actions to recover delinquent revenue or penalties. Not all anomalous transactions identified via DARTTS

[3] DARTTS contains financial transaction data obtained from the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN).

will result in enforcement action by HSI or CBP. Anomalous transactions are first researched to determine if they are in fact suspicious and warrant further inquiry. HSI and CBP personnel would gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination.

ICE is also expanding the use of DARTTS by permitting authorized users to access it from mobile devices. This will permit HSI and CBP users to conduct trade transparency analysis in DARTTS using government-furnished tablet computers and other mobile devices. This change allows DARTTS to be used in real-time enforcement encounters where accessing the system through a laptop or desktop government computer may be impractical or inefficient.

The expansion of DARTTS use to include select CBP personnel presents the risk that CBP users may have access to information in DARTTS that is in excess of what they need-to-know in order to perform their duties and CBP's mission. This risk was considered and mitigated by the creation of CBP-specific user roles which limit privileges within the system to only the categories of data that are pertinent to CBP's mission and enforcement authorities. As a result, CBP users will not have access to the financial transaction data in DARTTS, but will have access to the trade transaction and law enforcement data in the system.

There is also a risk that the aggregation of disparate data sets in DARTTS, including the law enforcement data sets, is inconsistent with the purpose(s) for which the data was originally collected. This risk is mitigated by limiting use of DARTTS to a very specific law enforcement purpose—to identify patterns and anomalies in trade and financial data that may be indicative of criminal or other illegal activity. The use of the trade and financial data in DARTTS 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. The use of the TECS and SDN List data in DARTTS is also consistent with the purposes of its collection. Both data sets are compiled for law enforcement purposes, and their use in a law enforcement system such as DARTTS is therefore consistent with the purposes of collection and appropriate.

Retention

ICE intends to request National Archives and Records Administration (NARA) approval to modify the DARTTS records retention schedule. Specifically, ICE will request to retain the data in DARTTS for ten years in the system, a change from the current 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 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 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.

Foreign DARTTS will also have a ten-year retention period for the data it maintains, which is separate from the primary DARTTS system. This retention period is based on a survey of the statutes of limitations of the nations that use Foreign DARTTS to support their own investigations into trade-based fraud.

ICE will also request to change the retention policy to ten years for the "inputs" to the DARTTS system, i.e., the original CD-ROMs, external storage devices or electronic data transfers containing raw data imported into DARTTS. Currently, the retention policy for the inputs is five years. This expanded retention period is necessary so that the inputs are retained for the same length of time that as the data in the DARTTS system, as described above, in case they are needed for data integrity and system maintenance/recovery purposes.

The expanded retention periods present no new privacy risks beyond those described in the DARTTS PIA. The risk that information may be retained for longer than necessary is mitigated by the fact that the ten year retention period 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 or other illegal activity. The ten year retention period ensures that sufficient information is available to conduct meaningful analyses for law enforcement purposes, while not keeping the information any longer than necessary.

Internal Sharing and Disclosure

As described above, ICE is expanding the use of DARTTS by granting select CBP officers and import specialists direct user access. These employees conduct trade transparency analysis in DARTTS in furtherance of CBP's mission to enforce U.S. trade laws and ensure the collection of all lawfully owed revenue from trade activities. Because CBP's enforcement authorities are not as broad as HSI's, CBP employees are assigned more restrictive user roles. CBP users are authorized to access trade and law enforcement data, but not financial transaction data, in DARTTS. CBP users access the DARTTS system via the secure ICE Network.

External Sharing and Disclosure

ICE is changing how foreign partners access U.S. trade data in DARTTS. ICE launched Foreign DARTTS, a separate web-based instance of the DARTTS system called that is specifically dedicated to the use of foreign government partners that operate trade transparency units and have signed customs mutual assistance agreements (or similar information sharing agreements) with the United States. Foreign DARTTS replaces the current method by which these partners use DARTTS, which involves stand-alone computers located in the foreign partner's office. These computers contain the DARTTS software and are loaded with anonymized U.S. trade data and the foreign partner's own trade data. ICE has supported the operation of these stand-alone DARTTS terminals by traveling to the foreign partner's office to update software and load new data into the system. To reduce costs and improve security, Foreign DARTTS was created to provide an Internet-based version of DARTTS hosted on the ICE network. In Foreign DARTTS, each foreign partner accesses only the data it is authorized to see as a result of user roles established in the system and managed by ICE. With Foreign DARTTS, there is no change in the data these foreign users can access or in the analytical tools available for their use.

Although it contains the same software, Foreign DARTTS is a completely separate system from DARTTS and does not contain all of the same data. Foreign DARTTS only contains trade data provided by the foreign partners that use the system, and the anonymized U.S. trade data that contains trade transactions between the United States and those foreign partners. Foreign DARTTS does not contain the U.S. financial transaction data or law enforcement data that is maintained in DARTTS. Foreign DARTTS relies on user roles to ensure that access privileges are enforced according to the information sharing agreements in place among the parties. Unless the countries have agreed to broader information sharing arrangements, the system will only permit foreign users to view their own nation's trade data and anonymized U.S. trade transactions between their nation and the United States. Foreign trade data is loaded into Foreign DARTTS after the foreign partner uploads the raw data to a secure FTP server at ICE. ICE formats the data and loads it into Foreign DARTTS and tags it so the system will be able to apply the appropriate user access rules to the data.

Notice

DHS is updating the DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN shortly after the publication of this update. There are no other changes to the notice procedures described in the DARTTS PIA.

Individual Access, Redress, and Correction

There are no changes to access, redress and correction procedures described in the DARTTS PIA. These procedures are also described in the DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, which is being amended and will be published in the Federal Register shortly after the publication of this update.

Technical Access and Security

Access to DARTTS is limited to HSI and CBP personnel with an established need-to-know related to their prescribed duties. A DARTTS user access request by an HSI or CBP employee must be approved by the employee's supervisor and submitted to the DARTTS Administrator, who is an HSI TTU employee designated by the TTU Unit Chief. User privileges are reviewed regularly to ensure that users are assigned the appropriate roles and those who no longer require access are removed from the access list. CBP officers using the system must be granted access to the ICE enterprise network so that they may access DARTTS. DARTTS authenticates users through the single-sign-on validation process on the ICE Network.

DARTTS has not presently been extended to a mobile platform, but ICE anticipates that the application vendor is researching that capability and will present that option for consideration in a future release. ICE currently employs robust mobile security controls to ensure that use of its various law enforcement tools, systems and data are protected when extended to mobile platforms. Examples of these controls include user access controls on the device, inactivity timeout device locking, and NIST validated encryption on the device contents (encrypted data at rest) and during transmission when communicating with the ICE Network and user applications thereon (data in transit). The same due diligence will be employed to ensure that DARTTS on a mobile platform does not compromise the security protections of the system or its data. Further, note that any plans to extend the DARTTS configuration to a mobile platform will only be for the domestic DARTTS application; there are no plans to provide that functionality to our foreign partners as a function of Foreign DARTTS.

The DARTTS intranet application resides on the ICE Network, is accessible via ICE standard user workstations, and inherits the user workstation and network component security controls from the ICE Application Infrastructure (AI) environment. Both the DARTTS and Foreign DARTTS applications and configurations are hosted in the secure DHS data center where support is provided for failures that interrupt basic services and other services related to system administration, storage management, patch management, vulnerability scanning, security monitoring, root cause analysis, change management, auditing, and production operations services.

Foreign DARTTS resides within a protected infrastructure space between the DHS Internet perimeter and the protected DHS/ICE internal network; this protected infrastructure space is also known as a network DMZ (demilitarized zone). Access to and use of the Foreign DARTTS system by our foreign partners will be restricted to that system component which resides in the DMZ, with no access beyond that to the domestic DARTTS system or any other internal network resources. The domestic DARTTS system and administrators will have access to the Foreign DARTTS system via separate connection from the internal ICE network.

A secure FTP site hosted on the Foreign DARTTS system is used by the foreign governments to upload their own foreign trade data that they want to provide the U.S. and to access in Foreign DARTTS. ICE retrieves the data from the site and formats it before loading it into DARTTS and Foreign DARTTS. When the data is loaded into Foreign DARTTS, it is tagged so the system knows which nation provided it and can identify that data and grant access to that government's users.

As described above, users of Foreign DARTTS have access to a more limited set of data than what is available to HSI and CBP users who access the primary DARTTS system. This limited access is enforced by user roles in Foreign DARTTS which are managed by the

DARTTS Administrator. User accounts are approved by the DARTTS Administrator; foreign governments do not have the authority to create or modify user accounts or privileges within Foreign DARTTS. Foreign DARTTS audit records produce sufficient information to determine the type of event, when and where the event occurred, the user causing the event and the outcome of the same. Furthermore, Foreign DARTTS users will be subject to data download restrictions thus limiting the amount of information they can pull out of the system. Upon reaching a pre-determine data amount, the user account will lock, forcing the user to contact the DARTTS system administrator for further action. This will provide HSI TTU with the opportunity to interview the user to determine the official/legitimate reason for the download as well as the nature of their investigation/research.

Foreign DARTTS users access the system on authorized foreign government computers using a digital certificate, signed by the DHS Certificate Authority (CA), on their computer that authorizes access to the Foreign DARTTS URL. The authenticity of the digital certificate is confirmed prior to granting the user access to the system. Once the digital certificate is authenticated, it is passed to Foreign DARTTS for further validation. Once the digital certificate passes validation, a unique user ID and password are required to gain access to Foreign DARTTS data. These security procedures prevent users from unauthorized computers and without proper user credentials from accessing Foreign DARTTS. SSL encryption is used to secure the transmission of data between the user's computer and the Foreign DARTTS system.

The risks of unauthorized access to and misuse of data contained in DARTTS are mitigated by the technological controls that limit user access to data and the use of audit mechanisms that log and monitor user activity. These risks are further mitigated by following DHS and government-wide security protocols that establish controls appropriate for the sensitive data contained in DARTTS, such as access controls, auditing, and user training. Additionally, foreign users access a completely separate system that contains only U.S. trade data limited to the scope of the existing international agreements and the information their governments provide to ICE. Users of Foreign DARTTS are also audited at the same level as domestic system users, and user authentication is ensured through robust security controls.

Technology

There are no changes to the DARTTS technology described in the DARTTS PIA that raise privacy concerns.

Responsible Official

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

Approval Signature

Final signed version on file with the DHS Privacy Office

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security