Privacy Impact Assessment
for the

FALCON-Roadrunner

DHS/ICE/PIA-040

November 12, 2014

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

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

Abstract

U.S. Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations (HSI) has deployed a new information system called FALCON-Roadrunner, which is a module of the larger HSI FALCON environment. This system generates investigative leads and conducts trend analysis that will be used to identify illicit procurement networks, terrorist groups, and hostile nations attempting to illegally obtain U.S. military products; sensitive dual-use technology; weapons of mass destruction (WMD); or chemical, biological, radiological, and nuclear materials. FALCON-Roadrunner gives HSI investigators and analysts the ability to perform research and generate leads for investigations of export violations within the jurisdiction of HSI. FALCON-Roadrunner analyzes trade, law enforcement, financial, and screening data across large, disparate datasets to identify statistically anomalous trade transactions that may warrant investigation of export violations. This PIA is necessary because FALCON-Roadrunner accesses and stores personally identifiable information (PII) retrieved from data systems owned by DHS and other government agencies, as well as commercially and publicly available data.

Overview

The HSI FALCON Environment

In 2012, ICE HSI created a new IT environment called "FALCON" to support ICE's law enforcement and criminal investigative missions. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other government applications and systems, while employing appropriate user access restrictions at the data element level and robust user auditing controls.

In February 2012, ICE deployed the first module of FALCON with the launch of FALCON Search & Analysis (FALCON-SA). FALCON-SA enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. ICE agents, criminal research specialists, and intelligence analysts use FALCON-SA to conduct research that supports the production of law enforcement intelligence products, provide lead information for investigative inquiry and follow-up, assist in the conduct of ICE criminal and administrative investigations, assist in the disruption of terrorist or other criminal activity, and discover previously unknown connections among existing ICE investigations. ICE's use of the system is always predicated on homeland security, law enforcement, and intelligence activities. FALCON-SA is an internal system used only by ICE.

In the FALCON general data storage environment, the data is aggregated with other FALCON data, and user access is controlled through a combination of data tagging, access control lists, and other technologies. Using a central data store for most FALCON data eliminates the need for multiple copies of the data. Foreign users are restricted from accessing any data that resides in the FALCON general data storage environment. Some law enforcement data used in FALCON-Roadrunner analyses is already stored in the FALCON general data storage environment.

For more information on the FALCON environment, please see the FALCON-SA PIA.[1] The FALCON-SA PIA Appendix will be updated to capture the FALCON-Roadrunner data that is being stored in the FALCON general data storage environment and made accessible to additional users through FALCON-SA's user interface.

FALCON-Roadrunner Overview

One of ICE's highest enforcement priorities is to prevent illicit procurement networks, terrorist groups, and hostile nations from illegally obtaining U.S. military products; sensitive dual-use technology[2]; weapons of mass destruction (WMD); or chemical, biological, radiological, and nuclear materials. The HSI Counter-Proliferation Investigations (CPI) Program oversees a broad range of investigative activities related to such violations of law. The CPI Program enforces U.S. laws governing the export of military items, controlled dual-use goods, firearms, and ammunition, as well as exports to sanctioned or embargoed countries.

FALCON-Roadrunner provides two services in support of HSI's CPI Program:

- Investigative Lead Generation: FALCON-Roadrunner allows CPI Unit investigators and analysts to generate leads for, and otherwise support, investigations of export violations within the jurisdiction of HSI. By using FALCON-Roadrunner to analyze trade data, CPI Unit investigators and analysts are able to identify anomalous transactions and activities that may be indicative of export violations and warrant investigation. Experienced HSI investigators independently confirm and further investigate these anomalies.
- Statistical/Trend Analysis: FALCON-Roadrunner provides export enforcement-related statistical reporting capabilities, derived from trade data that investigators access.

FALCON-Roadrunner Analytics

FALCON-Roadrunner allows users[3] to run complex search queries that assess massive volumes of trade transactions. These queries provide investigative leads and interdiction targets by identifying anomalies and non-obvious patterns and relationships within and across multiple large-scale trade, law enforcement, and other datasets. For example, FALCON-Roadrunner gives users the tools to work with multiple disparate data sets containing data elements of interest, and perform data filters or queries based on CPI-focused criteria, thereby reducing millions of records to a more manageable quantity that they can then further investigate. This process and use of technology provides for a more robust method to identify non-obvious relationships within very large quantities of data.

[1] See DHS/ICE/PIA-032 – FALCON Search & Analysis System (FALCON-SA), February 1, 2012, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_falconsa.pdf.
[2] Goods and technologies are considered to be dual-use when they can be used for both civil and military purposes, such as special materials, sensors and lasers, and high-end electronics.
[3] Throughout the body of this document, the term "user", shall be understood as meaning 'ICE HSI Counter-Proliferation Investigations (CPI) Unit investigators and analysts,' as it relates to FALCON-Roadrunner.

FALCON-Roadrunner will not predict future behavior or "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 transactions that are statistically anomalous based on user-specified queries. Once created by users, these queries can be shared with other users to allow them to benefit from queries that are found to be more useful or current. This results in a repeatable methodology whereby the queries are run periodically to see if and how patterns change in key trade areas. Users analyze these anomalies to identify suspicious transactions that warrant further investigation. If determined to warrant further investigation, HSI investigators gather additional information, verify the accuracy of the FALCON-Roadrunner data, and use human judgment and experience in deciding whether to investigate further. Not all anomalies lead to formal investigations. Individual results are used tactically to generate leads and larger scale changes in the results are used strategically to inform ICE's overall enforcement strategy in the CPI area.

FALCON-Roadrunner allows users to perform research and analyses that are not possible in any other ICE system because of the unique capabilities of the technology it uses, the data available for analysis, and the level of detail at which the data can be analyzed. As part of the CPI investigative process, FALCON-Roadrunner users are seeking to understand and assess the relationships between importers, exporters, manufacturers, commodity end-users, shippers, denied parties, licensing, export controls, and financing for each and every trade transaction to determine which are suspicious and warrant further investigation. If performed manually, this process would involve hours or even days of analysis of voluminous data and may not reveal potential violations due to the sheer volume and complexity of the data.

FALCON-Roadrunner is designed specifically to make this investigative process more efficient by leveraging advanced analytical technology designed to handle extremely large sets of complex data to identify anomalies and suspicious patterns/relationships. FALCON-Roadrunner is an analytical toolset specifically designed to rapidly process and analyze extremely large sets of data. These tools are connected to a data store (highly distributed file system) that ingests data from transactional databases and stores the data in a non-relational form. On ingestion, each data element is tagged and stored in a flat structure, which allows for greater parallel computation by the tools connected to the database and therefore provides a greater analytical capacity to identify non-obvious relationships. FALCON-Roadrunner will use this capacity to create and automatically apply repeatable, analytical search queries and processes to determine non-obvious, anomalous behaviors within the large-scale trade data. These search queries are not automated. Users have to input a command to return a result. The command can be repeated regularly, and a delta identified, but the user still needs to request when and how often a query needs to run. The system can check a hit list against a master data set and return back any matching entities, but there is no alert function.

FALCON-Roadrunner is owned and operated by the CPI Unit and made accessible to approved users via the ICE enterprise network. Only the HSI CPI Unit's investigators, analysts, and contractors are authorized to use the system. The results of Roadrunner analyses are forwarded to ICE HSI field offices as part of an investigative referral package to initiate or support a criminal investigation.

Interaction with FALCON-SA

FALCON-Roadrunner is an analytical tool over the larger FALCON environment. The datasets FALCON-Roadrunner analyzes are stored in the FALCON general data storage environment and are available to FALCON-Roadrunner users for additional analysis and investigation using the tools and additional data that is available in FALCON-SA. The data available to users through the FALCON-Roadrunner interface, however, is limited to only the datasets described in this PIA and does not include all datasets listed in the FALCON-SA PIA.

FALCON-SA system users without FALCON-Roadrunner privileges are able to view, access, and analyze data only as described in the FALCON-SA PIA and its appendices. Some of the data available to FALCON-Roadrunner users is also made available to FALCON-SA users, while other data will only be available in FALCON-SA if the user also has Roadrunner privileges. FALCON-SA enforces these access restrictions by requiring users with FALCON-Roadrunner privileges to designate their investigations within the system as CPI investigations; otherwise, the datasets specific to FALCON-Roadrunner will not be available for use and analysis in FALCON-SA. As discussed in Section 2.2, FALCON-Roadrunner adds new immigration, law enforcement, and publicly available data to the FALCON general data storage environment. ICE is updating the FALCON-SA PIA Appendix to reflect the new data that will be available via FALCON-SA as a result of the FALCON-Roadrunner system coming online.

FALCON-Roadrunner user rights and privileges are only granted to FALCON-SA system users who are ICE HSI CPI Unit investigators, analysts, and contractors with a need to know as a part of the performance of their official duties. Furthermore, FALCON-Roadrunner privileges are only granted by the FALCON system administrator with the explicit written permission of the FALCON-Roadrunner Program Manager.

Section 1.0 Authorities and Other Requirements

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

ICE is authorized to collect this information pursuant to: 6 U.S.C. § 236; 19 U.S.C. § 1589a; the Trade Act of 2002 § 343 (Note to 19 U.S.C. § 2071); 19 U.S.C. § 1484; 50 U.S.C. app. § 2411; 19 C.F.R. §§ 161.2 and 192.14; 31 U.S.C. § 5316; and 31 C.F.R. § 1010.340. HSI has the jurisdiction and authority to investigate violations involving the importation and exportation of merchandise into or out of the United States. Information analyzed by FALCON-Roadrunner supports, among other things, HSI's investigations into smuggling violations under 18 U.S.C. §§ 541, 542, 545, and 554; money laundering investigations under 18 U.S.C. §§ 1956, 1957, and 1960; and merchandise imported in non-compliance with 19 U.S.C. §§ 1481 and 1484.

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

The DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN applies to the information maintained in FALCON-Roadrunner.[4] Concurrently with the publication of this PIA, ICE is publishing an update to this SORN in the *Federal Register*. The DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN applies to the information maintained in FALCON-SA.[5]

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

A System Security Plan (SSP) has been completed for FALCON-SA. The latest Security Authorization for FALCON was granted on November 6, 2013. The FALCON-SA SSP also applies to FALCON-Roadrunner.

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

No. ICE is in the process of drafting a records retention schedule for NARA review. It will propose the retention and access periods for the FALCON environment as described in Section 5.1 below.

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

ICE does not collect PII directly from individuals or enterprises for use in FALCON-Roadrunner. All information is provided by other U.S. government agencies, commercial data sources, and foreign governments. Forms used by other U.S. government agencies to collect information have received OMB approval pursuant to the Paperwork Reduction Act. A complete listing of DHS forms and OMB Control numbers is below.

- U.S. Customs and Border Protection (CBP) 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

[4] DHS/ICE-005 - Trade Transparency Analysis and Research (TTAR), 77 FR 53893 (Sept. 4, 2012).
[5] DHS/ICE-006 - Intelligence Records System (IIRS), 75 FR 9233 (Mar. 1, 2010).

Section 2.0 Characterization of the Information

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

FALCON-Roadrunner uses various categories of data collected by other agencies, foreign governments, and commercial sources (hereafter referred to as "raw data"). This data contains the following PII, listed by category of information:

***U.S. Trade Data (Import / Export)*:** Names and addresses (home or business) of importers, exporters,[6] brokers, and consignees; importer, exporter, and broker identifications; and bill of lading data (i.e., data provided by carriers to confirm receipt and transportation of on-boarded cargo to U.S. Port), including consignee names and addresses, shipper names and addresses, container numbers, and carriers.

***Foreign Trade Data (Import / Export)*:** Names of importers, exporters, and brokers; addresses of importers and exporters; and importer, exporter, broker, and manufacturer identifications.[7]

***Screening Lists*:** Screening lists are produced by government entities and contain information on parties (individuals and entities) who are prohibited from engaging in certain trade transactions. Screening Lists contain some or all of the following PII: individual names, business names, addresses, dates of birth, places of birth, Social Security numbers (SSN), Taxpayer Identification Numbers (TIN), countries of citizenship, countries of residency, and passport numbers.

***Financial Data*:** U.S. and foreign financial transaction data that has been obtained through official investigations, legal processes, or legal settlements and may contain PII such as addresses, SSNs, and TINs, passport numbers and country of issuance, bank account numbers, transaction numbers, party names and addresses, and owner names and addresses.

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

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

***Law Enforcement Data*:** Data from DHS law enforcement systems that describe subjects of or witnesses in HSI investigations or ICE immigration enforcement actions, persons of interests to either ICE or CBP law enforcement personnel, applicants for U.S. visas who are screened by ICE, or those seeking a DHS-issued license (such as applicants for customs broker's licenses or to operate a customs bonded warehouse, be a bonded carrier, or bonded cartman). These records include some or all of the following PII: individual names, addresses, dates of birth, SSNs, TINs, passport numbers and countries of issuance, non-U.S. national identification number, Student and Exchange Visitor Information System (SEVIS) ID, bank account numbers, telephone numbers, driver's licenses and states of issuance, Alien Registration Numbers, business names, vehicle license plates, vehicle descriptions, vessel names, vessel descriptions, aircraft names, aircraft tail numbers, aircraft descriptions, and information about family members or associates of the individual.

Commercial Data: ICE uses the following commercial datasets in FALCON-Roadrunner:

The Risk Report is a commercially available counter-proliferation dataset used to screen commodity end-users, individuals, and other parties involved in a transaction against both denied parties (e.g., individuals and entities that have been denied export privileges) and profiles of risky entities developed and maintained by the Wisconsin Project on Nuclear Arms Control.[8] The Risk Report is a compendium of companies and individuals determined by the Wisconsin Project on Nuclear Arms Control to have some level of risk for illicit proliferation of nuclear technology, commodities, or weapons delivery systems. The Risk Report contains profiles of some 5,000 companies, government organizations, and people linked to the proliferation of nuclear, chemical, and biological weapons, missiles, and advanced military technology. The dataset contains some or all of the following PII: individual names, addresses, dates of birth, SSNs, and TINs.

The Industry and Sector Classifications Dataset contains business insights about a company based on the sectors in which the company participates through the sale of products and services, the company's interconnecting supply chain relationships, and the company's geographic revenue exposure.[9] The information is compiled by FactSet Research Systems, Inc. (FactSet) through publicly available press releases, investor presentations, corporate actions, and Internet queries. This dataset includes foreign corporate officers, addresses, and contact and ownership information associated with international businesses. This dataset contains some or all of the following PII: individual names, business names, and addresses.

[8] http://www.riskreport.org/.
[9] http://www.factset.com/data/company_data/industry_sector

Storage of the Data

The datasets listed above that are used, accessed, and analyzed by FALCON-Roadrunner are stored in FALCON's general data storage environment. In this environment, the data is aggregated with other FALCON data, and user access is controlled through a combination of data tagging, access control lists, and other technologies. Some of the data above is already maintained in the FALCON general data storage environment, specifically the law enforcement data, the financial data, the trade data, and one of the screening lists. The remaining datasets will be added upon the launch of FALCON-Roadrunner. Because FALCON-Roadrunner's analytical tools require the data to be structured in a non-relational form, a copy of the relevant data will be ingested into a non-relational data store (within the FALCON-SA environment) for use by the FALCON-Roadrunner tools. This strategy of centralized storage of FALCON data minimizes the replication of datasets in the same format that contain sensitive personal information, while centralized access controls within FALCON improve the consistency and efficiency of establishing and monitoring users' data access privileges.

Reports Generated by FALCON-Roadrunner

FALCON-Roadrunner uses analytical tools to create user-driven analyses of the raw data. These analyses focus on a variety of information, such as the activities of specific individuals and entities or trade data for particular commodities. The specific content and format of any particular analysis varies depending on the analytical tool selected and the parameters set by the user. The analysis may include high-level graphical representations that reveal shipping or receiving of suspicious packages related from or to various destinations worldwide; or listings of individuals or entities that are known or suspected to have engaged in criminal or other illegal activity.

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

All raw data used for FALCON-Roadrunner is provided by other U.S. government agencies, foreign governments, and commercial sources. ICE does not collect information directly from individuals or entities for use in FALCON-Roadrunner. Data that is already maintained in the FALCON general data storage environment has been noted below. All other data sources are new to FALCON. The specific raw data sources are:

***U.S. Trade Data*:** The data below is already maintained in the FALCON general data storage environment. The data is obtained from CBP as follows.

Import Data: Import data in the forms of extracts from CBP's Automated Commercial System,[10] which CBP collects from individuals and entities importing merchandise into the United States who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via the Automated Commercial Environment.

[10] *See* DHS/CBP/PIA-003(a) CBP's Automated Commercial System (ACS)/Automated Commercial Environment, *available at* www.dhs.gov/privacy.

Export Data: Export data in the form of Electronic Export Information (EEI)[11] that CBP collects from individuals and entities exporting merchandise from the United States.

***Foreign Trade Data*:** Import and export data provided to ICE by foreign law enforcement and customs officials pursuant to Customs Mutual Assistance Agreements (CMAA) or other similar information sharing agreements. Certain countries provide trade data that has been stripped of PII. Other countries provide complete trade data, including the names of businesses and individuals and other identifying information that may be contained in the trade records. This data is already maintained in the FALCON general data storage environment.

***Screening Lists*:** Screening list data is obtained from the following government sources:

European Union Denied Party Screening Lists:[12] A consolidated list of persons, groups, and entities subject to European Union (EU) financial sanctions.[13] This list is publicly available.

Consolidated U.S. Export Screening Lists:[14] A file that contains the consolidated export screening lists of the U.S. Departments of Commerce, State, and Treasury in one spreadsheet as an aide to industry in conducting electronic screens of potential parties to regulated transaction. The Consolidated Export Screening Lists are publicly available. The lists and their sources are as follows:

Department of Commerce – Bureau of Industry and Security (BIS)

- Denied Persons List:[15] Individuals and entities that have been denied export privileges. Any dealings with a party on this list that would violate the terms of its denial order are prohibited.
- Unverified List:[16] Commodity end-users that BIS has been unable to verify in prior transactions. The presence of a party on this list in a transaction is a "Red Flag" that should be resolved before proceeding with the transaction.
- Entity List:[17] Parties whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations (EAR). The list specifies the license requirements and policy that apply to each listed party.

---

[11] EEI is the export data as filed in the Automated Export System (AES). This data is the electronic equivalent of the export data formerly collected as Shipper's Export Declaration information. This information is now mandated to be filed through the AES or Automated Export System *Direct*. AES is operated jointly by the U.S. Census Bureau and CBP. *See* DHS/CBP/PIA-020 Export Information System (EIS), *available at* www.dhs.gov/privacy.

[12] *See* http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm.

[13] In order to facilitate the application of financial sanctions, the Banking Federation of the European Union, the European Savings Banks Group, the European Association of Co-operative Banks, the European Association of Public Banks (EU Credit Sector Federations), and the European Commission created an EU consolidated list of persons, groups, and entities subject to Common Foreign and Security Policy (CFSP) related financial sanctions. The consolidated list database was developed to assist the members of the EU Credit Sector Federations in their compliance with financial sanctions.

[14] *See* www.export.gov/ecr/eg_main_023148.asp.

[15] *See* http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list.

[16] *See* http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/unverified-list.

[17] *See* http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

Department of State – Bureau of International Security and Nonproliferation (ISN)

- Nonproliferation Sanctions:[18] Parties that have been sanctioned under various statutes. The linked webpage is updated as appropriate, but the *Federal Register* is the only official and complete listing of nonproliferation sanctions determinations.

Department of State – Directorate of Defense Trade Controls

- AECA Debarred List:[19] Entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services. Pursuant to the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), the AECA Debarred List includes persons convicted in court of violating or conspiring to violate the AECA and subject to "statutory debarment" or persons established to have violated the AECA in an administrative proceeding and subject to "administrative debarment."

Department of the Treasury – Office of Foreign Assets Control

- Specially Designated Nationals List (SDN):[20] A law enforcement dataset consisting of a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries as well as information about foreign individuals, groups, and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals," whose assets are blocked and U.S. persons and entities are generally prohibited from dealing with them. SDNs can be front companies, parastatal entities, or individuals determined to be owned or controlled by, or acting for or on behalf of, targeted countries or groups. SDNs also can be specially identified individuals such as terrorists or narcotics traffickers. This data is already maintained in the FALCON general data storage environment.

***Financial Data*:** Data collected by a government agency in the course of an official investigation, through legal processes, or through legal settlements and has been provided to ICE to deter international money laundering and related unlawful activities. For example, a court may direct a corporation to provide data to law enforcement agencies after determining that the corporation did not practice due diligence to deter money laundering or has facilitated criminal activities. This data is already maintained in the FALCON general data storage environment.

[18] *See* http://www.state.gov/t/isn/c15231.htm.
[19] *See* http://www.pmddtc.state.gov/compliance/debar_intro.html.
[20] *See* http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

Law Enforcement Data: This data is obtained from the following sources.

TECS Data: Subject records owned by CBP and ICE, and ICE investigative records obtained from CBP's TECS system. These records are already maintained in the FALCON general data storage environment via a system-to-system connection. TECS subject records include Person Subject, Vehicle Subject, Vessel Subject, Aircraft Subject, Thing Subject, Business Subject, and Organization Subject records. TECS investigative records concerning current or previous law enforcement investigations into violations of U.S. customs and immigration laws, as well as other laws and regulations within ICE's jurisdiction, including investigations led by other domestic or foreign agencies when ICE is providing support and assistance.[21] This data is already maintained in the FALCON general data storage environment.

Visa Security Data: The U.S. Department of State collects information directly from visa applicants as part of the visa application process. The data is then provided to DHS for security review, and is stored in ICE's VSPTS-Net system. It is ingested from VSPTS-Net into the FALCON general storage environment via a system to system connection.[22]

Commercial Data: The Risk Report commercial dataset is obtained through a subscription service with updates provided via a CD every two months. The data is uploaded from the CD into FALCON's general storage environment. The FactSet Industry and Sector Classifications commercial dataset is obtained through a subscription service. The data is received from the vendor every two months in CSV-formatted files and uploaded into the FALCON general data storage environment.

The refresh periods for the aforementioned data sources can be found in the Appendix, Table 2 – Source Data Refresh Periods. Information will be updated in the FALCON general storage environment during routine refreshes thereby ensuring accurate and current information as the old information is replaced with the newly refreshed information. Data collected by a government agency in the course of an official investigation, through legal processes, or through legal settlements may be retained for periods longer than the specified refresh periods.

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

Yes. FALCON-Roadrunner makes both publicly available and commercial data available to its users. ICE users of FALCON-Roadrunner use the publicly available screening lists produced by the U.S. government and EU to compare suspected trade and financial transactions against list members. ICE users research commonalities identified during comparison to determine if actual links exist between the list members for criminal investigative purposes.

---

[21] *See* DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative; DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy. *See also* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008).

[22] *See* DHS/ICE/PIA-011(a) Visa Security Program Tracking System-Network version 2.0 *available at* www.dhs.gov/privacy and DHS/ICE-012 Visa Security Program Records SORN, 74 FR 50228 (Sept. 30, 2009).

ICE users of FALCON-Roadrunner use the commercially available Risk Report to enhance FALCON-Roadrunner analysis and lead generation. The Risk Report is a compendium of companies and individuals determined by the Wisconsin Project on Nuclear Arms Control to have some level of risk for illicit proliferation of nuclear technology, commodities or weapons delivery systems. The Risk Report differs from government Consolidated Denied Parties Lists and other national or international denied parties lists in that those lists include only companies and individuals who have been adjudicated by governments for illegal export of controlled goods or technologies. The Risk Report aggregates lists of entities, companies and individuals for proliferation concerns who have not been adjudicated by national governments for proliferation violations but are determined by Wisconsin Project to be associated with proliferation activities.[23]

The commercially available FactSet Industry and Sector Classifications dataset is used to enhance lead generation. ICE will use this dataset to research concerning international corporations including ownership, trade transactions such as sales and purchase information, and corporate officer information. This information will be ingested into FALCON-Roadrunner to validate legitimate import/export transactions and to identify corporate affiliations to restricted and denied parties.

2.4 Discuss how accuracy of the data is ensured.

With the exception of ICE TECS records and visa security information, all information in FALCON-Roadrunner is obtained from other governmental organizations that collect the data under specific legislative authority or from commercial vendors. 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 FALCON-Roadrunner is highly accurate because the data was collected by third parties directly from the individual or entity to which the data pertains. In other instances, however, the data about individuals or entities is provided to the governmental organization by a third party. Commercial vendors are considered to have a financial incentive to provide high-quality and accurate data to their customers.

The system owner and users are aware that they cannot independently verify the accuracy of the bulk data the system receives. FALCON-Roadrunner is updated when corrected data is received from the collecting governmental organizations and commercial vendors. In the event that errors are discovered, the FALCON-Roadrunner system owner will notify the originator of the data. The system owner will remove datasets that are found over time to have poor data quality from FALCON-Roadrunner.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that data may be inaccurate or untimely because FALCON-Roadrunner relies on third-party data.

[23] http://www.riskreport.org/.

Mitigation: Much of the third-party data is publicly available and therefore individuals have the opportunity to view the data and could challenge its accuracy with the source. For example, the screening lists are produced by US and foreign government entities to identify individuals and entities that are precluded from being engaged in certain types of trade or financial transactions. By necessity, these lists are widely disseminated and publicly available online so they can be used by entities that are required to screen trade and financial transactions against them. In addition, the results of FALCON-Roadrunner analyses are used only as a starting point for the investigative process. Data relied upon in FALCON-Roadrunner must be verified by the investigator if it is to be used as evidence of a violation of law in criminal case.

Privacy Risk: There is a risk that incorrect information in the datasets used in FALCON-Roadrunner may be used to make decisions regarding individuals or entities.

Mitigation: This risk is mitigated by the fact that the system does not allow users to modify raw data received from the source systems, which reduces the potential for user-generated data errors. Additionally, CPI Unit investigators and analysts are prohibited from taking a law enforcement action against an individual or entity based on data and analysis from FALCON-Roadrunner alone. FALCON-Roadrunner is a system designed to help investigators generate leads for new or existing investigations. CPI investigators and analysts will fully investigate leads generated by FALCON-Roadrunner 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 obtains the needed information from the original data sources and further investigates the reason for the anomaly. If the anomaly can be legitimately explained, there is no need to further investigate for criminal violations. Any and all information obtained from FALCON-Roadrunner will be independently verified before it is acted upon or included in an ICE investigative or analytical report.

Privacy Risk: There is a risk that users may be impaired in their ability to assess data quality because the data is in aggregated form.

Mitigation: This risk is mitigated by the fact that FALCON-Roadrunner identifies for the user the source of each data element in the search results and analytical results. As trained CPI investigators and analysts, system users are already familiar with the quality of the various datasets in FALCON-Roadrunner and can use this information to analyze and weight the results generated by the system. It also enables users to identify data sources that might be contributing incorrect records or otherwise poor quality data, so the system owner can follow up with the data owner for correction or other appropriate remediation.

Privacy Risk: There is a risk that data may be inaccurate or untimely because of the intervals in which the sources issue updated data.

Mitigation: ICE updates the data available from external sources as soon as it is made available. Because these sources may issue updates on an infrequent or *ad hoc* basis, it is possible that the information used by FALCON-Roadrunner will not be current and therefore may be inaccurate. Because this system is used only to generate leads for investigations, the risk to privacy is low because any information used by the system will be independently verified by HSI agents before it is relied upon to take any enforcement action. Any data inaccuracies that may result from a lack of current data from these sources should be identified during the investigative process.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Trade Data: The PII contained in the trade data is used to identify the people who are involved in a transaction if a criminal violation is suspected. It is also used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects.

Financial Data: The PII contained in the financial data is used to identify the people involved in a transaction if a criminal violation is suspected. It is also used to conduct link analysis to identify relationships that may help identify suspicious transactions, witnesses, or suspects. SSNs may be used as unique identifier of an individual. For example, in FALCON-Roadrunner analysts can use a SSN as one of the parameters in a search and potentially find SSNs that are associated with more than one person. The results of these searches can lead to the discovery of potential criminal violations. SSNs are also used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects. Used in a similar way as SSNs, passport numbers are generally unique to an individual and are used to identify individuals. The passport numbers may be used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects. Finally, bank account information may be used to identify the bank or depository institution and the person involved in the transaction. It may also be used to conduct link analysis to identify relationships that may help identify suspect transactions, witnesses, or suspects.

Law Enforcement Data: The PII contained in the law enforcement data is used to determine whether an individual or entity being researched in FALCON-Roadrunner is part of an active, pending, or closed ICE HSI investigation or whether there is a CBP record. It is also used to identify international trade or financial transactions that are associated with a specially-designated individual or entity, which allows ICE HSI to take appropriate investigative actions in a timely and more efficient manner.

Screening Lists: The PII contained in screening lists is used to determine whether an individual or entity, which has previously been flagged for illicit or suspicious behavior, has engaged in further illicit actions related to counter proliferation investigations. For example, if an individual or entity listed as a Specially Designated National (SDN) by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) is found to be engaged in the export of a sensitive commodity through analysis done by the Roadrunner team, that individual could potentially be part of further investigation. Querying screening lists against trade data would allow for these connections to be made.

Commercial Data: The PII contained in the commercial datasets is used to identify trends and patterns in which foreign companies and individuals engage in order to procure sensitive technologies in an illicit manner. For example, private companies will often map the supply chain related to financial institutions in countries that are hostile to the United States. Analyzing that supply chain to see if anyone in that chain had previously participated in an export activity that included a sensitive technology would help identify if the activity warranted further investigation.

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

Yes. In response to user-specified queries, FALCON-Roadrunner uses technology to assist its users in identifying suspicious export transactions by analyzing trade data and identifying data that is statistically anomalous. Such anomalies can indicate export crimes that HSI is responsible for investigating. FALCON-Roadrunner will be able to match export and import transactions against these enriched data points from other datasets in order to identify anomalous transactions. Investigators follow up on anomalous exports to determine whether they are in fact suspicious and warrant further investigation. Not all anomalies lead to formal investigations.

FALCON-Roadrunner can also identify links between individuals 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 obtained during the course of an investigation, they can assist investigators in identifying potentially criminal activity and lead to identification of witness, other suspects, or additional suspicious transactions.

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

No. FALCON-Roadrunner is an internal system used only by ICE.

3.4 Privacy Impact Analysis: Related to the Uses of Information

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

Mitigation: As described in Section 3.3 of this document, security and access controls are in place to mitigate the risk of unauthorized individuals gaining access to PII. Access to FALCON-Roadrunner is limited to investigators and analysts who conduct official CPI activities. ICE personnel who are found to access or use the FALCON-Roadrunner 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 FALCON-Roadrunner analysis will, from that point forward, be carried out like any other criminal investigation. ICE will follow normal investigatory protocols and the same civil liberties and constitutional restrictions, such as the Fourth Amendment's probable cause requirements, will apply. CPI Unit investigators and analysts are prohibited from taking a law enforcement action against an individual or entity based on data and analysis from FALCON-Roadrunner alone. FALCON-Roadrunner is a system designed to help investigators generate leads for new or existing investigations. CPI investigators and analysts will fully investigate leads generated by FALCON-Roadrunner 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 obtains the needed information from the original data sources and further investigates the reason for the anomaly. If the anomaly can be legitimately explained, there is no need to further investigate for criminal violations. Any and all information obtained from FALCON-Roadrunner will be independently verified before it is acted upon or included in an ICE investigative or analytical report.

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

Mitigation: This risk is mitigated by limiting use of FALCON-Roadrunner to a very specific purpose – to identify patterns and anomalies in trade data that may be indicative of criminal activity – and limiting users to only those at ICE whose job responsibilities are focused on that purpose, specifically, the investigators and analysts within the CPI Unit. The system also prevents users from uploading additional data, limiting its usefulness for any investigations except those relating to CPI. The use of the data for this purpose is consistent with the original purpose for which it was collected, which is to enforce U.S. trade laws.

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

Mitigation: The risk of system misuse is minimized as user rights for FALCON-Roadrunner are limited to ICE HSI CPI Unit investigators and analysts with a need to know as a part of the performance of their official duties. In addition, the data that can be analyzed within the system is limited to the datasets described in this PIA and any subsequent updates; unlike FALCON-SA, users cannot upload ad hoc data into FALCON-Roadrunner for analysis. User

rights are granted on a requirements basis, meaning that the FALCON-Roadrunner Program Manager or an individual designated by the CPI Unit Chief grants users only the system functionality required of their position. In addition, FALCON-SA has a robust auditing feature that helps to identify and support accountability for user misconduct. User activity is audited heavily, extracting information from the system, resolving entities, searches, and viewing records. FALCON-Roadrunner audit logs will be maintained in FALCON-SA and auditing will be done by the FALCON-Roadrunner Program Manager in collaboration with the FALCON-SA Information System Security Officer (ISSO). HSI has also established controls that are based in policy, and when possible enforced by technology, that provide clear instruction on what the authorized uses of the system are. Disciplinary action for violations of HSI policies regarding the system is taken when warranted. Before receiving access to the system, all users are trained on system use and other policies governing the system. Lastly, FALCON-SA access controls are highly customizable and can be set at the record or even data field level. This ensures that users without a need to know are technically barred from accessing that information.

Section 4.0 Notice

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

ICE does not collect information directly from individuals or entities for use in FALCON-Roadrunner, 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 or through other forms of public notice, such as Privacy Act SORNs. A complete listing of the SORNs that apply to the raw data ICE receives from U.S. agencies for use in FALCON-Roadrunner can be found in the Appendix, Table 1 – Privacy Act System of Records Notices.

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

All information contained within FALCON-Roadrunner is collected by other government agencies or commercial vendors. The trade and financial information collected by U.S. agencies and foreign agencies is required by law to be provided to these agencies. For example, individuals and corporations may choose to not import to or export merchandise from the United States, but should they choose to undertake such trade activities, they must submit required information to the appropriate U.S. agency.

4.3 Privacy Impact Analysis: Related to Notice

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

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

Because FALCON-Roadrunner 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 and commercial vendors. ICE is not, therefore, in a position to provide notice or an opportunity to obtain consent from the individuals and entities from whom this information is collected. For that reason, specific notice and the opportunity to consent to these specific uses are not provided.

Section 5.0 Data Retention by the project

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

ICE intends to incorporate the retention periods for data accessible by FALCON-Roadrunner into the forthcoming records schedule for the FALCON environment. The data used by FALCON-Roadrunner will be accessed for ten years. Some of the data used by FALCON-Roadrunner is already maintained in the FALCON general data storage environment and subject to a proposed retention period; however, FALCON-Roadrunner will only access these existing datasets for ten years. Several new datasets are being added to the FALCON general storage environment with the launch of Roadrunner, and the retention and access period for those datasets is proposed to be ten years as well.

The ten-year retention and access period proposed for FALCON-Roadrunner is appropriate for the purpose of the system, which is to analyze current and historical trade and financial information to identify patterns and anomalies that may indicate criminal activity. Investigators typically do not need to access and analyze data that is more than ten years old to conduct the types of analyses described in this PIA. The ten-year retention and access period for FALCON-Roadrunner data ensures that sufficient information is available to conduct meaningful analyses for law enforcement purposes, while not keeping the information for any longer than is necessary or in a way that is inconsistent with the original purpose of the collection.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: The ten-year retention and access period proposed for FALCON-Roadrunner is appropriate for the purpose of the system, which is to analyze current and historical trade and financial information to identify patterns and anomalies that may indicate criminal activity. Investigators typically do not need to access and analyze data that is more than ten years old to conduct the types of analyses described in this PIA. The ten-year retention and access for FALCON-Roadrunner data ensures that sufficient information is available to conduct meaningful analyses for law enforcement purposes, while not keeping the information for any longer than is necessary or in a way that is inconsistent with the original purpose of the collection.

Section 6.0 Information Sharing

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

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

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

The DHS/ICE-005 TTAR SORN applies to FALCON-Roadrunner information and includes routine uses that permit external sharing for law enforcement, homeland and national security, audit, congressional, data breach, litigation, and records management purposes. The SORN also permits the sharing of U.S. trade data with foreign governments pursuant to Customs Mutual Assistance Agreements (CMAA) or other similar agreements to further enforcement efforts involving cargo safety and security, import and export smuggling, and related financial crimes. All external sharing is compatible with the law enforcement purpose for which ICE originally compiled and used this information.

6.3 Does the project place limitations on re-dissemination?

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

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

By policy and user training, users are instructed to record any disclosure of information outside of DHS by completing a disclosure form. A link to that form is provided in the FALCON-Roadrunner system and the form will be maintained in hard copy by the CPI Unit. FALCON-Roadrunner will include a disclosure reminder in the warning banner/rules of behavior that all users must acknowledge prior to system access. FALCON-Roadrunner will also contain a link to an external disclosure form that users must complete when making an external disclosure to comply with the accounting provisions of the Privacy Act, 5 U.S.C. § 552a(c). The form captures the date, nature, and purpose of the disclosure and the recipient's contact information.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: FALCON-Roadrunner users are required by law and policy, which is reinforced by user training, to share information from FALCON-Roadrunner with only those external partners who have a law enforcement, intelligence, or national security need to know. This requirement is in keeping with the law enforcement purpose of the system and the scope of ICE's mission as a law enforcement agency. FALCON-Roadrunner will include a disclosure reminder in the warning banner/rules of behavior that all users must acknowledge prior to system access. FALCON-Roadrunner will also contain a link to an external disclosure form that users must complete when making an external disclosure to comply with the accounting provisions of the Privacy Act, 5 U.S.C. § 552a(c).

Section 7.0 Redress

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

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

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

All or some of the requested information may be exempt from access pursuant to the Privacy Act, 5 U.S.C. § 552a, in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in FALCON-Roadrunner 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.[24]

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

The correction procedures are identical to those described in Section 7.1 above. All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in FALCON-Roadrunner 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.[25]

[24] *See* 74 FR 38887 (Aug. 5, 2009).
[25] *See* 74 FR 38887 (Aug. 5, 2009).

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

The information about correction is made available through the publication of this PIA and the associated SORNs. Because FALCON-Roadrunner contains copies of datasets owned by DHS components and offices or other agencies, individuals may also have the option to seek access to and correction of their data directly from those agencies or offices that originally collected it (see Appendix Table 2). Information that is corrected in the original source system will be updated in the FALCON general storage environment during routine refreshes thereby ensuring accurate and current information.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: Because the data in this system may originate from other systems of records with a law enforcement purpose, individuals' rights to be notified of the existence of data about them, and to direct how that data may be used by HSI, are limited. As such, this risk cannot be fully mitigated. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system.

Because this system makes use of several publicly available and commercial datasets that are described in this PIA, individuals are able to determine if information about them is included in those datasets. For example, individuals included on a publicly available screening list of prohibited parties, such as the Treasury Department's Specially Designated Nationals List, could determine that information about them exists in FALCON-Roadrunner. Individuals may contact the commercial provider of the data for redress purposes.

Section 8.0 Auditing and Accountability

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

As mentioned before, FALCON-Roadrunner is a component system of the larger HSI FALCON environment. As a result, FALCON-Roadrunner uses the same access controls, user auditing, and accountability as those described in the FALCON-SA PIA. For more information on these, please see the FALCON-SA PIA.[26]

[26] *See* DHS/ICE/PIA-032 – FALCON Search & Analysis System (FALCON-SA), February 1, 2012,

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

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

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

FALCON-Roadrunner user rights and privileges are only granted to FALCON-SA system users who are ICE HSI CPI Unit investigators, analysts, and contractors with a need to know as a part of the performance of their official duties. Furthermore, FALCON-Roadrunner privileges are only granted by the FALCON system administrator with the explicit written permission of the FALCON-Roadrunner Program Manager. FALCON-Roadrunner privileges are evaluated on a case-by-case basis.

FALCON-Roadrunner is used by ICE HSI CPI Unit investigators and analysts. FALCON-Roadrunner user rights and privileges are only granted to FALCON-SA system users who are ICE HSI CPI Unit investigators, analysts, and contractors with a need to know as a part of the performance of their official duties. Furthermore, FALCON-Roadrunner privileges are only granted by the FALCON system administrator with the explicit written permission of the FALCON-Roadrunner Program Manager. FALCON-Roadrunner privileges are evaluated on a case-by-case basis

Currently FALCON-Roadrunner has three user roles:

(1) FALCON-Roadrunner ICE User: Investigates financial or trade transactions, conducts analysis, and generates reports.
(2) FALCON-Roadrunner ICE Supervisor: Investigates financial or trade transactions, conducts analysis, generates reports, and assigns user roles.
(3) FALCON-SA ICE Administrator: Creates, activates, revokes, and/or removes user access and accounts for the FALCON environment and applications as a whole.

Assigned user 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. All ICE FALCON-Roadrunner users are able to access only data that is associated with the user's specific profile.

---

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_falconsa.pdf.

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

ICE established a governance process to: monitor the ongoing operations of FALCON environment; decide requests to add new data sources to the system; expand user privileges to other DHS components or other agencies; and establish policies and procedures that govern system operation and user behavior. The governance process is staffed by HSI leadership and senior managers, and advisory services are provided by the ICE Office of the Principal Legal Advisor and the ICE Privacy Office. This governance process will help to ensure that any proposals for new data sharing arrangements are appropriately vetted for legal and privacy risks, as well as compliance with the DHS Fair Information Practice Principles. In addition, formal written agreements between ICE and other agencies to share data or provide access to FALCON-Roadrunner would be reviewed by the ICE Privacy Office and Office of Principal Legal Advisor as a matter of routine. Also, the routine ingestion of data from any new source will require an update to the Appendix of this PIA and approval from the DHS Chief Privacy Officer.

Responsible Officials

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

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Table 1. Privacy Act System of Records Notices (SORNs)

Agencies	Systems of Records Notices
CBP	DHS/CBP-015 Automated Commercial System (ACS) SORN, 73 FR 77759 (Dec. 19, 2008)
	DHS/CBP-001 Automated Commercial Environment/International Trade Data System (ACE/ITDS) SORN, 71 FR 3109 (Jan. 19, 2006)
	DHS/CBP-011 TECS SORN, 73 FR 77778, (Dec. 19, 2008)
ICE	DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, 77 FR 53893 (Sept. 4, 2012)
	DHS/ICE-006 ICE Intelligence Records System (IIRS) System of Records Notice, 75 FR 9233 (Mar. 1, 2010)
	DHS/ICE-012 Visa Security Program Records SORN, 74 FR 50228 (Sept. 30, 2009)

Table 2. Source Data Refresh Periods

Sources of Information	Category of Information	Refresh Period
Trade Data		
U.S. Customs and Border Protection (CBP)	Automated Commercial System (ACS) Import Data	Daily
	Automated Export System (AES) Export Data	
Foreign Government Partners	Foreign Trade Data	Monthly
Screening Lists		
Departments of Commerce, State, and the Treasury	Consolidated Export Screening Lists	Daily
U.S. Department of the Treasury Office of Foreign Assets Control (OFAC)	Specially Designated Nationals List (SDN)	Monthly
European Union (EU)	European Union Denied Party Screening Lists	When obtained
Financial Data		
Other Federal, State, and Local Law Enforcement Agencies	Other Financial Data	When obtained
Law Enforcement Data		
CBP	TECS Subject and Investigative Records	Daily
U.S. Immigration and Customs Enforcement (ICE)	Visa Security Information	Daily
Other Commercially and Publicly Available Data		
Wisconsin Project on Nuclear Arms Control	The Risk Report	Bi-monthly
FactSet Research Systems, Inc.	Industry and Sector Classifications	When obtained