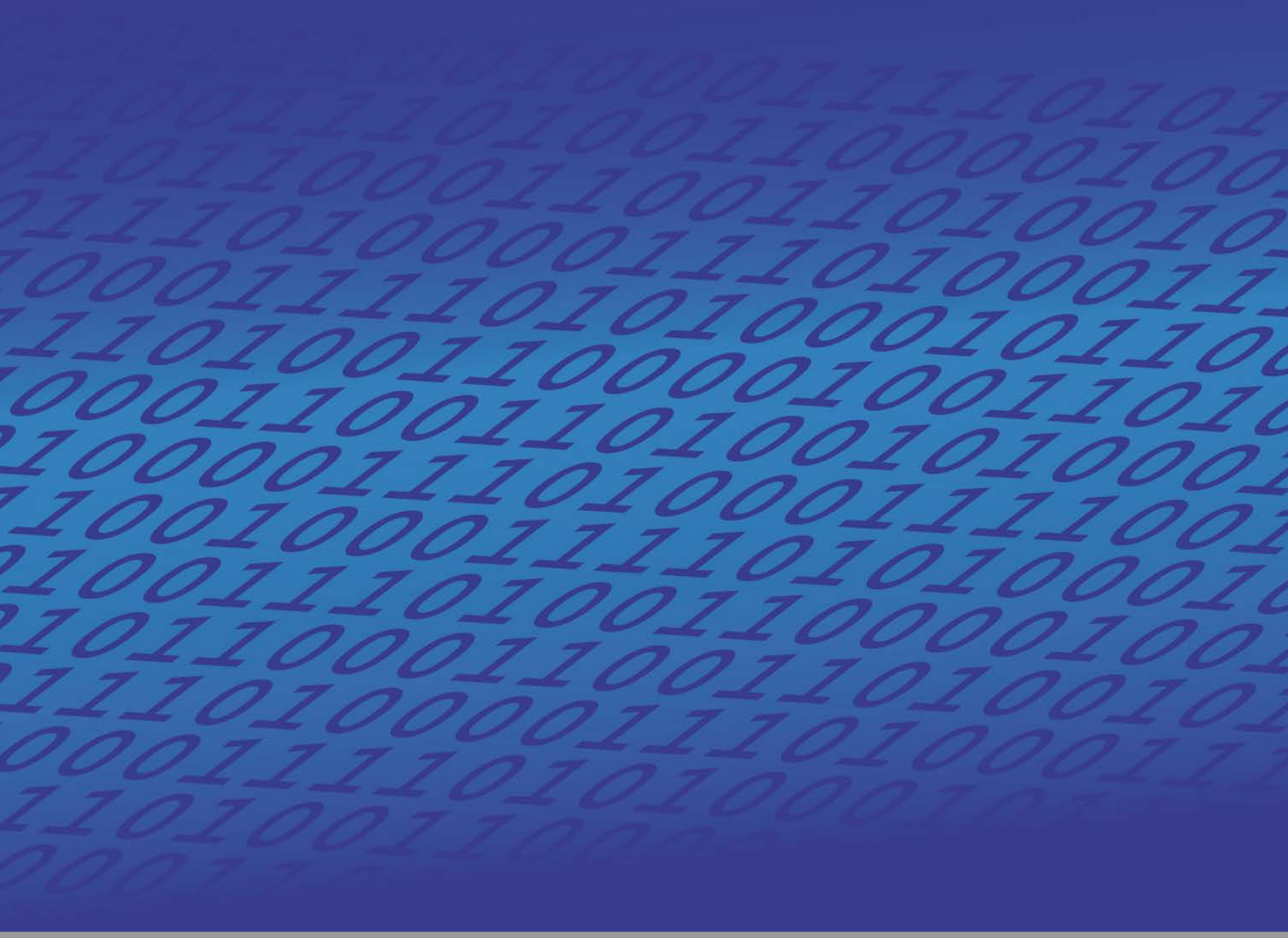

Department of Homeland Security

Privacy Office

2013 Data Mining Report to Congress

February 2014

Homeland Security

FOREWORD

February 2014

I am pleased to present the Department of Homeland Security's (DHS) 2013 Data Mining Report to Congress. The Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3, requires DHS to report annually to Congress on DHS activities that meet the Act's definition of data mining.

For each identified activity, the Act requires DHS to provide the following: (1) a thorough description of the activity and the technology and methodology used; (2) the sources of data used; (3) an analysis of the activity's efficacy; (4) the legal authorities supporting the activity; and (5) an analysis of the activity's impact on privacy and the protections in place to protect privacy. This is the eighth comprehensive DHS Data Mining Report and the sixth report prepared pursuant to the Act. Two annexes to this report, which include Law Enforcement Sensitive information and Sensitive Security Information, respectively, are being provided separately to Congress as required by the Act.

With the creation of DHS, Congress authorized the Department to engage in data mining and the use of other analytical tools in furtherance of Departmental goals and objectives. Consistent with the rigorous compliance process it applies to all DHS programs and systems, the DHS Privacy Office has worked closely with the programs discussed in this report to ensure that they employ data mining in a manner that both supports the Department's mission to protect the homeland and protects privacy.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Joseph R. Biden
President, U.S. Senate

The Honorable John Boehner
Speaker, U.S. House of Representatives

The Honorable Thomas R. Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn, M.D.
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Charles Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Saxby Chambliss
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Michael McCaul
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Darrell Issa
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Robert W. Goodlatte
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Mike Rogers
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable C. A. Dutch Ruppersberger
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Inquiries relating to this report may be directed to the DHS Office of Legislative Affairs at 202-447-5890.

Sincerely,

Karen L. Neuman
Chief Privacy Officer
U.S. Department of Homeland Security

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) Privacy Office (DHS Privacy Office or Office) is providing this report to Congress pursuant to Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), entitled the Federal Agency Data Mining Reporting Act of 2007 (Data Mining Reporting Act or the Act).[1] This report discusses activities currently deployed or under development in the Department that meet the Data Mining Reporting Act's definition of data mining, and provides the information set out in the Act's reporting requirements for data mining activities.

In the 2012 DHS Data Mining Report,[2] the DHS Privacy Office discussed the following Department programs that engage in data mining, as defined by the Data Mining Reporting Act:

(1) The Automated Targeting System (ATS), which is administered by U.S. Customs and Border Protection (CBP) and includes modules for inbound (ATS-N) and outbound (ATS-AT) cargo, land border crossings (ATS-L), and passengers (ATS-P);

(2) The Analytical Framework for Intelligence (AFI), which is administered by CBP; and

(3) The Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by U.S. Immigration and Customs Enforcement (ICE).

This year's report, covering the period January 1, 2013, through December 31, 2013, provides updates on modifications, additions, and other developments that have occurred in the current reporting year including use of ATS by DHS components other than CBP. The report also presents two new programs currently in development that will include data mining capabilities: the DHS Data Framework, a DHS-wide pilot initiative, and FALCON-Roadrunner, which is administered by ICE. Additional information on DARTTS and on the Transportation Security Administration's (TSA) Secure Flight Program's use of ATS is being provided separately to Congress in two annexes to this report that contain Law Enforcement Sensitive Information and Sensitive Security Information, respectively.

The Homeland Security Act of 2002, as amended (Homeland Security Act), expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[3] DHS exercises its authority to engage in data mining in the programs discussed in this report, all of which the DHS Chief Privacy Officer has reviewed for potential impact on privacy. The Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974, as amended (Privacy Act);[4] the E-Government Act of 2002 (E-Government Act);[5] and Section 222 of the Homeland Security Act, which states that the Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."[6]

[1] 42 U.S.C. § 2000ee-3.
[2] http://www.dhs.gov/sites/default/files/publications/privacy/Reports/2012-data-mining-report-to-congress.pdf.
[3] 6 U.S.C. § 121(d)(14).
[4] 5 U.S.C. § 552a.
[5] Pub. L. No. 107-347.
[6] 6 U.S.C. § 142(a)(1).

The DHS Privacy Office's privacy compliance policies and procedures are based on a set of eight Fair Information Practice Principles (FIPPs) that are rooted in the tenets of the Privacy Act. The FIPPs have served as DHS's core privacy framework since the Department was established. They are memorialized in the Privacy Office's *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*[7] and in Department-wide management directives including, most recently, Directive 047-01, *Privacy Policy and Compliance* (July 2011).[8] The Office applies the FIPPs to the full breadth and diversity of information and interactions within DHS, including DHS activities that involve data mining.

As described more fully below, the DHS Privacy Office's compliance process requires systems and programs using Personally Identifiable Information (PII) and other information relating to individuals to complete federally-mandated privacy documentation consisting of a Privacy Impact Assessment (PIA), as required by the E-Government Act,[9] and a System of Records Notice (SORN), as required by the Privacy Act,[10] before they become operational. All programs discussed in this report have either issued new or updated PIAs or are in the process of doing so; all are also covered by SORNs.

While each program described below engages to some extent in data mining, none makes decisions about individuals solely on the basis of data mining results. In all cases, DHS employees conduct investigations to verify (or disprove) the results of data mining, and then bring their own judgment and experience to bear in making determinations about individuals initially identified through data mining activities. The DHS Privacy Office has worked closely with each of these programs to ensure that required privacy compliance documentation is current, that personnel receive appropriate privacy training, and that privacy protections have been implemented.

[7] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[8] Directive 047-01 and its accompanying Instruction are available at https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf and https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-instruction-047-01-001.pdf, respectively. Directive 047-01 is available at http://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf. The Directive supersedes DHS Directive 0470.2, *Privacy Act Compliance*, which was issued in October 2005.
[9] Pub. L. No. 107-347.
[10] 5 U.S.C. § 552a(e)(4).

DHS PRIVACY OFFICE
2013
DATA MINING REPORT

Table of Contents

I. LEGISLATIVE LANGUAGE

The Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3, includes the following requirement:

(c) Reports on data mining activities by Federal agencies

(1) Requirement for report - The head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made available to the public, except for an annex described in subparagraph (3).

(2) Content of report - Each report submitted under subparagraph (A) shall include, for each activity to use or develop data mining, the following information:

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

(C) A thorough description of the data sources that are being or will be used.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to—

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.[11]

The Act defines "data mining" as:

a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where—

[11] 42 U.S.C. § 2000ee-3(c).

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;
(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program;

or

(ii) the security of a Government computer system.[12]

[12] 42 U.S.C. § 2000ee-3(b)(1). "[E]lectronic telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources" are not "databases" under the Act. 42 U.S.C. § 2000ee-3(b)(2). Therefore, searches, queries, and analyses conducted solely in these resources are not "data mining" for purposes the Act's reporting requirement. Two aspects of the Act's definition of "data mining" are worth emphasizing. First, the definition is limited to pattern-based electronic searches, queries, or analyses. Activities that use only PII or other terms specific to individuals (e.g., a license plate number) as search terms are excluded from the definition. Second, the definition is limited to searches, queries, or analyses that are conducted for the purpose of identifying predictive patterns or anomalies that are indicative of terrorist or criminal activity by an individual or individuals. Research in electronic databases that produces only a summary of historical trends, therefore, is not "data mining" under the Act.

II. DATA MINING AND THE DHS PRIVACY COMPLIANCE PROCESS

The Department of Homeland Security (DHS) Privacy Office (DHS Privacy Office or Office) is the first statutorily mandated privacy office in the Federal Government. Its mission is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. The Office works to minimize the impact of DHS programs on an individual's privacy, particularly an individual's personal information, while achieving the Department's mission to protect the homeland. The Chief Privacy Officer reports directly to the Secretary of Homeland Security, and the Office's mission and authority are founded upon the responsibilities set forth in Section 222 of the Homeland Security Act of 2002, as amended (Homeland Security Act).[13]

This is the DHS Privacy Office's eighth comprehensive report to Congress on DHS activities that involve data mining and the sixth report pursuant to the Federal Agency Data Mining Report Act of 2007 (Data Mining Reporting Act).[14] The Homeland Security Act expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[15] DHS exercises this authority to engage in data mining in the programs discussed in this report, all of which have been reviewed by the Chief Privacy Officer for potential impacts on privacy. The DHS Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974, as amended (Privacy Act);[16] the E-Government Act of 2002 (E-Government Act);[17] and Section 222 of the Homeland Security Act, which states that the DHS Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."[18] The Office's compliance process discussed below is designed to identify and mitigate risks to privacy that may be posed by any DHS program, project, or information technology system.

The DHS Privacy Office's privacy compliance policies and procedures are based on the Fair Information Practice Principles (FIPPs), which are rooted in the tenets of the Privacy Act. The

[13] 6 U.S.C. § 142. The authorities and responsibilities of the Chief Privacy Officer were last amended by the 9/11 Commission Act on August 3, 2007. The 9/11 Commission Act added investigative authority, the power to issue subpoenas to non-Federal entities, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under Section 222 of the Homeland Security Act. These responsibilities are further described on the DHS Privacy Office website (http://www.dhs.gov/privacy) and in the *DHS Privacy Office 2013 Annual Report to Congress*, available at http://www.dhs.gov/sites/default/files/publications/2013-dhs-privacy-office-annual-report-final-11062013.pdf.

[14] 42 U.S.C. § 2000ee-3. All of the DHS Privacy Office's Data Mining Reports are available on the DHS Privacy Office website at http://www.dhs.gov/privacy.

[15] The Act states that, "[s]ubject to the direction and control of the Secretary, the responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection, shall be as follows . . . To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate." 6 U.S.C. § 121(d)(13).

[16] 5 U.S.C. § 552a.

[17] Pub. L. No. 107-347.

[18] 6 U.S.C. § 142(a)(1).

FIPPs have served as DHS's core privacy framework since the Department was established. They are memorialized in the Privacy Office's *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*[19] and in Department-wide management directives including, most recently, Directive 047-01, *Privacy Policy and Compliance* (July 2011).[20] The FIPPs govern the appropriate use of Personally Identifiable Information (PII) at the Department. DHS uses the FIPPs to enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it fulfills the Department's mission to preserve, protect, and secure the homeland. The Office applies the FIPPs to the full breadth and diversity of Department systems and programs that use PII, including DHS activities that involve data mining.

DHS uses three primary documents to conduct privacy compliance: (1) the Privacy Threshold Analysis (PTA); (2) the Privacy Impact Assessment (PIA);[21] and (3) the System of Records Notice (SORN).[22] While each of these documents has a distinct function in the privacy compliance framework at DHS, together they further the transparency of Department activities and demonstrate accountability.

- **PTAs:** The PTA is the first document completed by a DHS Component or office seeking to implement or modify a system, program, technology, project, or rulemaking. The PTA identifies whether the system, program, technology, project, or rulemaking is privacy-sensitive and thus requires additional privacy compliance documentation such as a PIA or SORN.
- **PIAs:** PIAs examine the privacy impact of information technology (IT) systems, programs, technologies, projects, or rulemakings. PIAs allow the DHS Privacy Office's Compliance Group to review system management activities in key areas such as security and how information is collected, used, and shared. If a PIA is required, the DHS Component will draft the PIA for review by the Component privacy officer or privacy point of contact (PPOC) and component counsel. Part of the PIA analysis includes determining whether an existing SORN appropriately covers the activity or a new SORN is required. Once the PIA is approved at the Component level, the Component privacy officer or PPOC submits it to the DHS Privacy Office Compliance Group for review and approval by the Chief Privacy Officer.
- **SORNs:** SORNs provide notice to the public regarding Privacy Act information collected by DHS and maintained in a department system of records. SORNs also provide notice regarding how information is used, retained, and may be accessed or corrected. Part of the Privacy Act analysis requires determining whether to apply certain Privacy Act exemptions

[19] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[20] Directive 047-01 and its accompanying Instruction are available at https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf and https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-instruction-047-01-001.pdf, respectively. The Directive supersedes the DHS Directive 0470.2, *Privacy Act Compliance*, which was issued in October 2005.
[21] The E-Government Act mandates PIAs for all federal agencies when there are new electronic collections of, or new technologies applied to, PII. Pub. L. No. 107-347. As a matter of policy, DHS extends this requirement to all programs, systems, and activities that involve PII or are otherwise privacy-sensitive.
[22] The Privacy Act requires federal agencies to publish SORNs for any group of records under agency control from which information is retrieved by the name of an individual or by an identifying number, symbol, or other identifier assigned to the individual. 5 U.S.C. § 552a(a)(5) and (e)(4).

to limit access to records by an individual for law enforcement or national security reasons. If a SORN is required, the program manager works with the Component privacy officer or PPOC and Component counsel to write a SORN and submits it to the DHS Privacy Office Compliance Group for review and approval by the Chief Privacy Officer.

PTAs, PIAs, and SORNs serve the common purpose of identifying and documenting areas of privacy focus for programs, IT systems, and collections of PII.[23]

After privacy compliance documentation has been completed and a program, system, or initiative is operational, the DHS Privacy Office also has the authority to monitor and verify ongoing compliance through a Privacy Compliance Review (PCR) conducted by the Office's Oversight Group. Consistent with the Office's unique role as both an advisory and an oversight body for the Department's privacy-sensitive programs and systems, the PCR is designed as a constructive mechanism for improving compliance with assurances made in existing PIAs, SORNs, or Information Sharing Access Agreements or similar agreements. Department PIAs increasingly include a PCR requirement, to demonstrate the Department's commitment to ongoing monitoring of privacy compliance. For example, U.S. Customs and Border Protection (CBP) and the Privacy Office issued a PIA for CBP's Analytical Framework for Intelligence (AFI), discussed below in Section IV.B of this report, which requires that a PCR be completed within 12 months of AFI's deployment. The Privacy Office initiated the AFI PCR in August 2013, and the PCR was ongoing as the reporting period for this report ended.

The DHS Privacy Office identifies DHS programs that engage in data mining through several processes in addition to its routine compliance oversight activities. The Office reviews all of the Department's Exhibit 300 budget submissions to the Office of Management and Budget (OMB) to learn of programs or systems that use PII and to determine whether they address privacy appropriately.[24] The Office uses the PTA to review all information technology systems that are going through the security authorization process required by the Federal Information Security Management Act of 2002 (FISMA)[25] to determine whether they maintain PII. The PIA process also provides the Office insight into technologies used or intended to be used by DHS. These oversight activities provide the Office opportunities to learn about proposed data mining activities and to engage program managers in discussions about potential privacy issues.

The DHS Privacy Office has worked closely with the relevant DHS Components to ensure that privacy compliance documentation required for each program described in this report is current.

[23] Once the PTA, PIA, and SORN are completed, the documents are periodically scheduled for a mandatory review by the DHS Privacy Office (timing varies by document type). For systems that require only PTAs and PIAs, the review process begins again three years after the document is complete or when there is an update to the program, whichever is earlier. The process begins with either the update or submission of a new PTA. The Office of Management and Budget (OMB) Privacy Act guidance in OMB Circular A-130 requires that SORNs be reviewed on a biennial basis.

[24] All major DHS IT programs are reviewed by the DHS Privacy Office Compliance Group on an annual basis, prior to submission to OMB for inclusion in the President's annual budget. The Compliance Group plays a substantial role in the review of the OMB budget submissions (known as Exhibit 300s) prior to submission to OMB. *See* Office of Mgmt. & Budget, Executive Office of the President, OMB Circular No. A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, available at http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s300.pdf.

[25] Title 44, U.S.C., Chapter 35, Subchapter III (Information Security).

All of these programs have either issued new or updated PIAs or are in the process of doing so; all are also covered by SORNs.

III. REPORTING: NEW PROGRAMS

During this reporting period, the DHS Privacy Office identified two new programs currently in development that will include data mining capabilities: the DHS Data Framework, a DHS-wide pilot initiative, and FALCON-Roadrunner, which is administered by U.S. Immigration and Customs Enforcement (ICE).

A. DHS Data Framework

DHS is developing the DHS Data Framework, a scalable information technology program with built-in capabilities to support advanced data architecture and governance processes. This program will alleviate mission limitations associated with stove-piped IT systems that are currently deployed across multiple operational components in DHS. It will also enable more controlled, effective, and efficient use and sharing of available homeland security-related information across the DHS enterprise and, as appropriate, the U.S. Government, while protecting privacy. DHS is conducting three pilots to test different capabilities needed to implement the Framework: the Neptune Pilot, the Common Entity Index Prototype (CEI Prototype), and the Cerberus Pilot. The data to be used in the pilots is discussed below. The Privacy Office and program officials have issued PIAs for each of these pilots and for the DHS Data Framework as a whole.[26]

DHS is changing the way it structures its information architecture and data governance to further consolidate information in a manner that protects individuals' privacy, civil rights, and civil liberties. Existing information maintained by the Department is subject to privacy, civil rights and civil liberties, and other legal and policy protections, and it is collected under different authorities and for various purposes. The existing architecture of DHS databases, however, is not conducive to effective implementation of the "One DHS" policy, which was implemented to afford DHS personnel timely access to relevant and necessary homeland-security information they need to successfully perform their duties and protect the Homeland.[27] Currently, this access is cumbersome, time-intensive, and requires personnel to log on and query separate databases in order to determine what information DHS systems contain about a particular individual. The goal of the DHS Data Framework is to provide a user the ability to search an amalgamation of data extracted from multiple DHS systems for a specific purpose and to view the information in a clear and accessible format. The DHS Data Framework will enable efficient and cost-effective searches across DHS databases in both classified and unclassified domains.

[26] The Neptune Pilot PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-neptune-09252013.pdf. The CEI Prototype PIA is available at http://www.dhs.gov/publication/dhsallpia-046-2-common-entity-index-prototype. The Cerberus Pilot PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-cerberus-nov2013.pdf. The DHS Data Framework PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

[27] *DHS Policy for Internal Information Exchange and Sharing*, February 1, 2007. Under this policy, DHS personnel requesting information maintained within another departmental component may access such information when the requestor (1) has an authorized purpose, mission, and need-to-know before accessing the information in performance of his or her duties; (2) possesses the requisite background or security clearance; and (3) assures adequate safeguarding and protection of the information.

The DHS Data Framework defines four elements for controlling data:

(1) *User attributes* identify characteristics about the user requesting access such as organization, clearance, and training;

(2) *Data tags* label the data with the type of data involved, where the data originated, and when it was ingested;

(3) *Context* combines what type of search and analysis can be conducted (function), with the purpose for which data can be used (authorized purpose); and

(4) *Dynamic access control* policies evaluate user attributes, data tags, and context to grant or deny access to DHS data in the repository based on legal authorities and appropriate policies of the Department.

DHS will log activities of participants in the pilots to aid audit and oversight functions.

Initially, the data tags, context, and dynamic access will be tested to enable greater information sharing and comparison in support of operations and to build in greater privacy protections. The DHS Data Framework will incorporate a User Attribute Hub, which will maintain a listing of a system user's attributes for determining access control (e.g., component in which the individual works, location, job series). This attribute hub is being developed through a different effort by the DHS Office of the Chief Information Officer. The following capabilities will test the other three elements of the Framework using data from the CBP Electronic System for Travel Authorization (ESTA),[28] the ICE Student and Exchange Visitor Information Systems (SEVIS),[29] and the Transportation Security Administration (TSA) Alien Flight Student Program (AFSP).[30]

- ***Neptune Pilot:*** The Neptune Pilot, residing in the Sensitive but Unclassified/For Official Use Only (SBU/FOUO) domain, will ingest and tag data in a data repository known as "Neptune." This pilot will test the second element of the DHS Data Framework (data tags). Data in the Neptune Pilot will be shared with the CEI Prototype and the Cerberus Pilot, but will ***not*** be accessible for other purposes.
- ***CEI Prototype:*** The CEI Prototype, also residing on the SBU/FOUO domain, will receive a subset of the tagged data from the Neptune Pilot and correlate data from across component datasets. The CEI Prototype will test the utility of the Neptune-tagged data—specifically, the ability to ensure that only users with certain attributes are able to access data based on defined purposes using the dynamic access control process. This prototype will use data tags to test the third and fourth elements of the DHS Data Framework (context and dynamic access control, respectively).
- ***Cerberus Pilot:*** The Cerberus Pilot, residing in the Top Secret/Sensitive Compartmented Information (TS/SCI) domain, will receive all of the tagged data from the Neptune Pilot in a separate data repository known as Cerberus. The Cerberus Pilot will test the ability to ensure that only users with certain attributes are able to access data based on defined

[28] *See* DHS/CBP/PIA-007(c), ESTA Update, June 5, 2013; DHS/CBP/PIA-007(b) ESTA - Internet Protocol Address and System of Records Notice Update, July 18, 2012; DHS/CBP/PIA-007(a) ESTA Fee and Information Sharing Update, July 18, 2011; DHS/CBP/PIA-007 ESTA June 2, 2008, available at www.dhs.gov/privacy.
[29] *See* DHS/ICE/PIA-001(a) SEVIS Update National Counter Terrorism Center, June 23, 2011; DHS/ICE/PIA-001 – SEVIS, February 5, 2005, available at www.dhs.gov/privacy.
[30] DHS/TSA/PIA-026 AFSP, December 4, 2009, available at www.dhs.gov/privacy.

purposes using the dynamic access control process. This pilot will leverage the data tags to test the context and dynamic access control elements of the DHS Data Framework. The Cerberus Pilot will also test the ability to perform simple and complex searches across different component datasets using different analytical tools.

During the pilot phase of the DHS Data Framework, several different types of search tools and analytical capabilities will be tested. The planned search capabilities include pattern-based searches designed to identify previously unknown individuals who pose threats to homeland security.

The DHS Privacy Office has been intensively involved in the development of these capabilities and in the DHS Data Framework as a whole since its inception. The Privacy Office will evaluate the need for updated PIAs and continue to be involved in the development of the governance structure for the Framework. In future Data Mining Reports the Office will provide further details on the DHS Data Framework as it becomes operational.

B. FALCON-Roadrunner

ICE is currently developing FALCON-Roadrunner, a system that will enable ICE Homeland Security Investigations Counter-Proliferation Investigations Unit (HSI CPIU) investigators and analysts to perform research and generate leads for investigations of export violations within the jurisdiction of HSI. It will also provide HSI CPIU users the ability to run search queries and perform analytics across large, disparate trade, financial, law enforcement, and other commercially and publicly available datasets using an efficient, accurate, and user-driven methodology. FALCON-Roadrunner will be deployed within ICE's existing FALCON environment, which is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other federal, state, local, and foreign government and private sector sources, with appropriate user access restrictions and robust user auditing controls.[31]

The datasets analyzed by FALCON-Roadrunner will primarily consist of export data, import data, financial data, law enforcement data, and other commercially and publicly available data. When fully deployed, the ingestion, mapping, and presentation tools incorporated into FALCON-Roadrunner will facilitate and enhance an investigator's ability to join disparate datasets provided by other government applications and systems, perform search and analysis on the disparate datasets, and provide reports and leads. HSI CPIU users will have the ability to perform research and analyses not possible in any other ICE system because of the data FALCON-Roadrunner contains, the technology used to leverage the data, and the analytical models developed by HSI CPIU to drive the search and analysis technology. The uniqueness of the system lies in its ability to permit HSI CPIU investigators and analysts the capability to easily

[31] In February 2012, ICE deployed the first module of FALCON with the launch of FALCON Search & Analysis (FALCON-SA). FALCON-SA provides the capability to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. For more information on the FALCON environment, *see* DHS/ICE/PIA-032A FALCON Search & Analysis System (FALCON-SA), January 16, 2014, http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf.

join previously disparate datasets and then filter the data to identify entities of interest. Filtered data can be represented in the form of graphs, charts, and other visual graphics.

In addition to HSI CPIU lead generation, FALCON-Roadrunner will perform statistical analytics and trend analysis for HSI CPIU and the Export Enforcement Coordination Center. FALCON-Roadrunner will provide export enforcement statistical research capabilities within export and import data. This statistical-analytic function will discern, describe, and document trends within export/import datasets for entities associated with proliferation, licensing, and enforcement in order to inform ICE decision makers. The underlying technology used in FALCON-Roadrunner will allow for more efficient and accurate statistical modeling and analysis of large, disparate datasets, in a more user-friendly manner than previously available at ICE.

User access to FALCON-Roadrunner will be restricted at the dataset level, and stringent auditing of system access will be in place to ensure appropriate usage of the system.

Initial deployment of FALCON-Roadrunner is currently scheduled for the third quarter of Fiscal Year (FY) 2014. The DHS Privacy Office and ICE were conducting a PIA and SORN update for FALCON-Roadrunner as the reporting period for this report ended. In future Data Mining Reports, the Privacy Office will provide additional information on FALCON-Roadrunner as it becomes operational.

IV. REPORTING: PROGRAM UPDATES

In the 2012 DHS Data Mining Report,[32] the DHS Privacy Office discussed the following Department programs that engage in data mining, as defined by the Data Mining Reporting Act:

(1) The Automated Targeting System (ATS), which is administered by CBP and includes modules for inbound (ATS-N) and outbound (ATS-AT) cargo, land border crossings (ATS-L), and passengers (ATS-P);

(2) The Analytical Framework for Intelligence (AFI), which is administered by CBP; and

(3) The Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by ICE.

This section of the 2013 report presents complete descriptions of these programs together with updates on modifications, additions, and other developments that have occurred in the current reporting year, including use of ATS by DHS components other than CBP.

[32] http://www.dhs.gov/sites/default/files/publications/privacy/Reports/2012-data-mining-report-to-congress.pdf.

A. Automated Targeting System (ATS)

1. 2013 Program Update

a) Non-Immigrant and Immigrant Visa Applications

As described in the 2012 PIA,[33] ATS-P is used to vet non-immigrant visa applications for the U.S. Department of State (DoS). In spring 2014, CBP and DoS will begin pre-adjudication investigative screening and vetting for immigrant visas. DoS sends online visa application data to ATS-P for pre-adjudication investigative screening. ATS-P vets the visa application and provides a response to the DoS's Consular Consolidated Database (CCD) indicating whether or not DHS has identified derogatory information about the individual. Applications of individuals for whom derogatory information is identified through ATS-P are either vetted directly in ATS-P if a disposition can be determined without further investigation or additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net) case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD. The Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA) (Pub. L. 107-173), specifically 8 U.S.C. § 1721, authorizes the use of ATS-P for screening non-immigrant and immigrant visas.

b) Overstay Vetting

In April 2013, Phase 2 of the One DHS Overstay Vetting effort went live with the new Visa Overstay Hotlist. The Overstay Hotlist is a list of overstay candidates derived from data obtained through ATS to develop priorities based on associated risk patterns related to national security and public safety. This prioritized list of overstay candidates is then passed on to ICE's LeadTrac[34] system for further investigation and possible enforcement action. In addition to prioritizing overstay candidates, ATS is also used to vet arrival and departure information received from the Arrival and Departure Information System (ADIS)[35] to identify potential additional information on visa overstay candidates based on supporting data available through ATS, i.e., border crossing information (BCI), Form I-94 Notice of Arrival/Departure records, and data from SEVIS.

[33] The ATS PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.
[34] LeadTrac is an immigration status violator database that is used by the Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit at ICE. The primary function of LeadTrac is to identify and track nonimmigrant visitors to the United States who overstay their period of admission or otherwise violate the terms of admission. The identities of potential violators are then sent to ICE field offices for appropriate enforcement action. LeadTrac is covered by the DHS/ICE-009 - External Investigations SORN, available at http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31269.htm. The LeadTrac database is being updated and is scheduled to deploy in the first quarter of FY 2015. A new PIA is being drafted and will be published prior to LeadTrac's deployment.
[35] The PIA for ADIS is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf, and the SORN for ADIS is available at http://www.gpo.gov/fdsys/pkg/FR-2007-08-22/html/E7-16473.htm.

As with the Phase 1 Pilot, discussed in the 2012 Data Mining Report,[36] Phase 2 also uses overstay data obtained through system processing in ATS-P and ADIS to identify certain individuals who have remained in the United States beyond their authorized period of admission (overstays) and who may present a heightened security risk. The Department continued the Pilot and began implementing long term solutions during the course of this reporting year. Pursuant to the Consolidated and Further Continuing Appropriations Act, 2013 (enacted on March 26, 2013), ADIS is now being managed by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program's successor organization, the Office of Biometric Identity Management in the DHS National Protection and Programs Directorate. The goal of the Overstay Vetting effort is to allow ICE to deploy its investigative resources efficiently to locate high-risk overstays and initiate criminal investigations or removal proceedings against those individuals. ADIS provides biographical information on identified and possible overstays to CBP, to be run in ATS-P against risk-based rules based on information derived from past investigations and intelligence. CBP returns the results of these analyses to ADIS, which, in turn, provides them to ICE for further processing. These activities are covered by PIAs for ATS[37] and the US-VISIT Technical Reconciliation Analysis Classification System[38] and Overstay Vetting.[39]

The legal authorities for the One DHS Overstay Vetting Pilot include: the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000, Public Law 106–215; the Visa Waiver Permanent Program Act of 2000, Public Law 106–396; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Public Law 107–56; EBSVERA; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53.[40]

2. Special ATS Programs

a) ATS Enhancements to Watchkeeper System

Watchkeeper is the United States Coast Guard's (USCG) information sharing and management system software for Interagency Operations Centers (IOC). USCG established Watchkeeper to improve multi-agency maritime security operations and enhance cooperation among partner agencies at the nation's 35 most critical ports. Watchkeeper coordinates and organizes port security information to improve tactical decision-making, situational awareness, operations monitoring, rules-based processing, and joint planning in a coordinated interagency environment. Additionally, Watchkeeper provides a shared operational picture, shared mission tasking, and shared response information sets to all users within an IOC, including partner federal agencies and local port partners.

[36] 2012 Data Mining Report at p. 6.
[37] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.
[38] See DHS/NPPD/USVISIT/PIA-004 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_tracs.pdf.
[39] The DHS Overstay Vetting Pilot PIA was issued on December 29, 2011, to add another layer of analysis to this process that can be updated as the program matures. The PIA lists all of the SORNs applicable to this program, and is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_odovp.pdf.
[40] A complete list of authorities is included in the PIA for the Overstay Vetting Pilot.

USCG has enhanced Watchkeeper by integrating the ATS-N and ATS-P modules discussed below as tools to conduct pre-arrival screening and vetting of vessel cargo, crew, and passengers, and plans to move the program to operational status in 2014. The ATS-enhanced Watchkeeper will provide near real-time data for Captains of the Port (COTP) to better evaluate threats and deploy resources through the active collection of incoming vessel information. With a more detailed picture of the risk profile that a vessel presents, COTPs can make appropriate, informed decisions well ahead of the vessel's arrival in port. USCG legal authorities for the ATS-Enhanced Watchkeeper system include the Security and Accountability for Every Port (SAFE Port) Act of 2006, 46 U.S.C. § 70107A; 5 U.S.C. § 301; 14 U.S.C. § 632; 33 U.S.C. §§ 1223, 1226; 46 U.S.C. §§ 3717, 12501; Section 102 of the Maritime Transportation Security Act of 2002, Pub. L. No. 108-274; Section 102(c) of the Homeland Security Act, 14 U.S.C. § 2; 33 C.F.R. part 160; and 36 C.F.R. chapter XII. The DHS Privacy Office and USCG published a PIA for Watchkeeper on January 4, 2013.[41]

b) Secure Flight

During this reporting period, TSA's Secure Flight Program (Secure Flight) continued to leverage real-time, threat-based intelligence rules run by ATS-P to identify individuals requiring enhanced screening prior to boarding an aircraft. On the basis of those rules, Secure Flight transmits to the airlines instructions identifying such individuals. More information about Secure Flight is included in the Secure Flight PIA, which was updated most recently on September 4, 2013.[42] An annex to this report containing Sensitive Security Information (SSI) about Secure Flight's use of ATS-P is being provided separately to the Congress. TSA's legal authorities related to passenger screening include 49 U.S.C. § 114(d), (e), and (f), and Section 4012(a) of Public Law 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)).

c) Air Cargo Advance Screening Pilot

During this reporting period, CBP and TSA continued to conduct the Air Cargo Advance Screening (ACAS) joint pilot discussed in the 2012 Data Mining Report,[43] using existing CBP data collections and ATS-N to identify pre-departure air cargo that may pose a threat to aviation. In October 2013, CBP extended the pilot through July 26, 2014.[44] TSA targeting personnel work side-by-side with CBP targeting personnel to jointly develop rules designed to address threats from air cargo and to review data in ATS. TSA legal authorities for this pilot include 49 U.S.C. § 114(f)(10), which authorizes TSA to ensure the adequacy of security measures for the transportation of cargo, and Section 1602 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), which amended 49 U.S.C. § 44901 to authorize TSA to screen cargo on passenger and all-cargo aircraft.

3. General ATS Program Description

CBP developed ATS, an intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. ATS compares traveler, cargo, and conveyance

[41] http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_uscg_watchkeeper_20130104.pdf.
[42] https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf.
[43] 2012 Data Mining Report at p. 7.
[44] 78 F.R. 63237 (Oct. 23, 2013), available at https://www.federalregister.gov/a/2013-24856.

information against intelligence and other enforcement data by incorporating risk-based targeting rules and assessments. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. CBP also uses ATS to identify other potential violations of U.S. laws that CBP enforces. In this way, ATS allows CBP officers charged with enforcing U.S. law and preventing terrorism and other crimes to focus their efforts on the travelers, conveyances, and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Traveler, conveyance, and shipment data are processed through ATS and are subject to a real-time, rules-based evaluation.

ATS consists of five modules that focus on exports, imports, passengers and crew (airline passengers and crew on international flights, and passengers and crew on sea carriers), private vehicles crossing at land borders, and a workspace to support the creation and retention of analytical reports. This report discusses all of these modules: ATS-N and ATS-AT (both of which involve the analysis of cargo), ATS-L (which involves analysis of information about vehicles and their passengers crossing the land border), ATS-P (which involves analysis of information about certain travelers), and the ATS Targeting Framework (ATS-TF) (a platform for temporary and permanent storage of data).

The U.S. Customs Service, a legacy organization of CBP, traditionally employed computerized tools to target potentially high-risk cargo entering, exiting, and transiting the United States. ATS was originally designed as a rules-based program to identify such cargo; it did not apply to travelers. ATS-N and ATS-AT became operational in 1997. ATS-P became operational in 1999 and is now critically important to CBP's mission. ATS-P allows CBP officers to determine whether a variety of potential risk indicators exist for travelers or their itineraries that may warrant additional scrutiny. ATS-P maintains Passenger Name Record (PNR) data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from certain air carriers in 1997. Currently, CBP collects this information to the extent it is collected by carriers in connection with a flight into or out of the United States, as part of CBP's border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).[45]

ATS ingests various data in real-time from the following DHS and CBP systems: the Automated Commercial System (ACS), the Automated Manifest System (AMS), the Advance Passenger Information System (APIS), the Automated Export System (AES), the Automated Commercial Environment (ACE), ESTA, the Nonimmigrant Information System (NIIS), DHS BCI, SEVIS, and TECS. TECS includes information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[46] Terrorist Screening Database (TSDB) and provides access to the

[45] 49 U.S.C. § 44909. The regulations implementing ATSA are codified at 19 C.F.R. § 122.49d.

[46] The TSC is an entity established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the FBI, established the TSC pursuant to Homeland Security Presidential Directive 6, which required the Attorney General to establish an organization to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful

Department of Justice's (DOJ) National Crime Information Center (NCIC), which contains information about individuals with outstanding wants and warrants, and to Nlets, a clearinghouse for state wants and warrants as well as information from state Departments of Motor Vehicles (DMV). ATS collects PNR data directly from air carriers. ATS also collects data from certain airlines and express consignment services in ATS-N. ATS accesses data from these sources, which collectively include: electronically filed bills of lading (i.e., forms provided by carriers to confirm the receipt and transportation of on-boarded cargo to U.S. ports), entries, and entry summaries for cargo imports; Electronic Export Information (EEI) (formerly referred to as Shippers' Export Declarations) submitted to AES and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land border crossing and referral records for vehicles crossing the border; airline reservation data; non-immigrant entry records; records from secondary referrals, incident logs, and suspect and violator indices; seizures; and information from the TSDB and other government databases regarding individuals with outstanding wants and warrants and other high-risk entities.[47]

In addition to providing a risk-based assessment system, ATS provides a graphical user interface for many of the underlying legacy systems from which ATS pulls information. This interface improves the user experience by providing the same functionality in a more rigidly controlled access environment than the underlying system. Access to this functionality of ATS uses existing technical security and privacy safeguards associated with the underlying systems.

A large number of rules are included in the ATS modules that encapsulate sophisticated concepts of business activity that help identify potentially suspicious behavior. The ATS rules are constantly evolving to meet new threats and refine existing rules. When evaluating risk, ATS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups.

a) ATS-Inbound (ATS-N) and ATS-Outbound (ATS-AT) Modules

i. Program Description

ATS-N assists CBP officers in identifying and selecting for intensive inspection inbound cargo shipments that pose a high risk of containing weapons of mass effect, illegal narcotics, or other contraband. ATS-N is available to CBP officers at all major ports of entry (i.e., air, land, sea, and rail) and also assists CBP personnel in the Container Security Initiative and Secure Freight Initiative decision-making processes.

ATS-AT aids CBP officers in identifying exports that pose a high risk of containing goods requiring specific export licenses, illegal narcotics, smuggled currency, stolen vehicles or other contraband, or exports that may otherwise violate U.S. law. ATS-AT sorts EEI data extracted from AES, compares it to a set of rules, and evaluates it in a comprehensive fashion. This information assists CBP officers in targeting or identifying exports that pose potential aviation

use of terrorist information in screening and law enforcement processes. The TSC maintains the Federal Government's consolidated terrorist watch list, known as the TSDB.

[47] The 2012 Data Mining report noted ATS's use of data from Dun & Bradstreet, a commercially available data source, to assist with company identification though name and address matching. 2012 Data Mining Report at p. 8. ATS no longer uses data from Dun & Bradstreet, and CBP has determined that a replacement for this data is no longer necessary.

safety and security risks (e.g., hazardous materials) or may be otherwise exported in violation of U.S. law.

ATS-N and ATS-AT examine data related to cargo in real time and engage in data mining to provide decision support analysis for the targeting of cargo for suspicious activity. The cargo analysis provided by ATS is intended to add automated anomaly detection to CBP's existing targeting capabilities, to enhance screening of cargo prior to its entry into the United States.

ii. Technology and Methodology

ATS-N and ATS-AT do not collect information directly from individuals. The data used in the development, testing, and operation of ATS-N and ATS-AT screening technology is taken from bills of lading and shipping manifest data provided to CBP through AMS, ACS, ACE, and AES by entities engaged in international trade as part of the existing cargo screening process. The results of queries, searches, and analyses conducted in the ATS-N and ATS-AT system are used to identify anomalous business behavior, data inconsistencies, abnormal business patterns, and potentially suspicious business activity generally. No decisions about individuals are made solely on the basis of these results.

The SAFE Port Act requires ATS to use or investigate the use of advanced algorithms in support of its mission.[48] To that end, as discussed in previous DHS Data Mining Reports, ATS established an Advanced Targeting Initiative, which employs the development of data mining, machine learning,[49] and other analytic techniques to enhance ATS-N and ATS-AT. This Initiative strives to improve law enforcement capabilities with predictive models and establish performance evaluation measures to assess the effectiveness of ATS screening of for inbound and outbound cargo shipments across multimodal conveyances.

Current efforts seek to augment existing predictive models by expanding the use of feedback from identified travel patterns and seizure data. CBP officers and agents use these models to assist them in identifying pattern elements in data collected from the trading and traveling public, and use this information to make determinations regarding examination and clearance. Additionally, CBP continues to develop and test machine learning models or knowledge engineered scenario based rules to target specific threats. These system enhancements principally incorporate programming enhancements to automate successful user (manual) practices for broader use and dissemination by ATS users nationally. They are an attempt to share, broadly and more quickly, best practices to enhance targeting efforts across the CBP mission.

The Advanced Targeting Initiative is part of ATS's maintenance and operation of the ATS-N and ATS-AT systems. The design and tool-selection processes for data mining, pattern recognition, and machine learning techniques under development in the Advanced Targeting Initiative are being evaluated through user acceptance testing by the National Targeting Center (NTC). The NTC and CBP Office of Intelligence and Investigative Liaison (OIIL) further support the

[48] 6 U.S.C. § 901.

[49] Machine learning is concerned with the design and development of algorithms and techniques that allow computers to "learn." The major focus of machine learning research is to extract information from data automatically, using computational and statistical methods. This extracted information may then be generalized into rules and patterns.

performance of research on entities and individuals of interest, data queries, data manipulation on large and complex datasets, data management, link analysis, social network analysis,[50] and statistical analysis in support of law enforcement and intelligence operations. Upon successful testing, the programming enhancements are included in maintenance and design updates to system operations and deployed on the national level to provide a more uniform enhancement to CBP operations. This practice will continue to be incorporated into future maintenance protocols for ATS.

iii. Data Sources

As noted above, ATS-N and ATS-AT do not collect information directly from individuals. The information is either submitted by private entities and initially collected in DHS/CBP source systems (i.e., ACE, ACS) in accordance with U.S. legal documentation requirements (e.g., sea, rail, and air manifests), is created by ATS as part of its risk assessments and associated rules, or is received from a foreign government pursuant to a Memorandum of Understanding and Interconnection Security Agreement.

ATS-N and ATS-AT use the information from source databases to gather information about importers and exporters, cargo, and conveyances used to facilitate the importation of cargo into and the exportation of cargo out of the United States. This information includes PII concerning individuals associated with imported and exported cargo (e.g., brokers, carriers, shippers, buyers, sellers, exporters, freight forwarders, and crew). ATS-N receives data pertaining to entries and manifests from ACS and ACE, and processes it against a variety of rules to make a rapid, automated assessment of the risk of each import.[51] ATS-AT uses EEI data that exporters file electronically with AES, export manifest data from AES, and export airway bills of lading to assist in formulating risk assessments for cargo bound for destinations outside the United States.

CBP uses commercial off-the-shelf (COTS) software tools to graphically present entity-related information that may represent terrorist or criminal activity, to discover non-obvious relationships across cargo data, to retrieve information from ATS source systems to expose unknown or anomalous activity, and to conduct statistical modeling of cargo-related activities as another method to detect anomalous behavior. CBP also uses custom-designed software to resolve ambiguities in trade entity identification related to inbound and outbound cargo.

iv. Efficacy

Based upon the results of testing and operations in the field, ATS-N and ATS-AT have proved to be effective means of identifying suspicious cargo that requires further investigation by CBP

[50] Social network analysis is a method of ascertaining entity relationships within existing data to assist analysts in predictive modeling, researching targeted individuals or organizations, and visualization of targeted entities.

[51] ATS-N collects information from source systems regarding individuals in connection with the following items including: Sea/Rail Manifests from AMS; Cargo Selectivity Entries and Entry Summaries from the Automated Broker Interface, a component of ACS; Air Manifests (bills of lading) from AMS; Express Consignment Services (bills of lading); Manifests (bills of lading from Canada Customs and Revenue); CBP Automated Forms Entry Systems CBP Form 7512; QP Manifest Inbound (bills of lading) from AMS; Truck Manifests from ACE; Inbound Data (bills of lading) from AMS; entries subject to Food and Drug Administration Prior Notice requirements from ACS; and Census Import Data from the U.S. Department of Commerce.

officers. The results of ATS-N and ATS-AT analyses identifying cargo as suspicious have been regularly corroborated by physical searches of the identified cargo.

The goal of the Advanced Targeting Initiative is to enhance CBP officers' ability to identify entities such as organizations, cargo, vehicles, and conveyances with a possible association to terrorism. Leads resulting in a positive, factual determination obtained through further investigation and physical inspections of cargo demonstrate the efficacy of the technologies used in the Initiative. Additionally, successful user acceptance testing has enabled CBP to incorporate certain of these technological enhancements, designed to automate formerly manual practices by CBP officers, into uniform system upgrades to expand the scope of results from past successful practices.

v. Laws and Regulations

There are numerous customs and related authorities authorizing the collection of data regarding the import and export of cargo as well as the entry and exit of conveyances.[52] ATS-AT and ATS-N also support functions mandated by Title VII of Public Law 104-208 (1996 Omnibus Consolidated Appropriations Act for FY 1997), which provides funding for counterterrorism and drug law enforcement. ATS-AT also supports functions arising from the Anti-Terrorism Act of 1987[53] and the 1996 Clinger-Cohen Act.[54] The risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.[55]

b) ATS-Passenger Module (ATS-P)

i. Program Description

ATS-P is a custom-designed system used at U.S. ports of entry, particularly those receiving international flights and voyages (both commercial and private), and the CBP NTC to evaluate passengers and crew members prior to their arrival to or departure from the United States. ATS-P facilitates the CBP officer's decision-making process about whether a passenger or crew member should receive additional inspection prior to entry into, or departure from, the country because that person may pose a greater risk for terrorism and related crimes or other crimes. ATS-P is a fully operational application that utilizes CBP's System Engineering Life Cycle methodology[56] and is subject to recurring systems maintenance.

[52] *See, e.g.*, 19 U.S.C. §§ 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; 22 U.S.C § 401; and 46 U.S.C. § 46501.
[53] 22 U.S.C. § 5201 *et seq.*
[54] 40 U.S.C. § 1401 *et seq.*
[55] 6 U.S.C. § 912(b).
[56] CBP's Office of Information & Technology's System Engineering Life Cycle (SELC) is a policy that lays out the documentation requirements for all CBP information technology projects, pilots, and prototypes. All projects and system changes must have disciplined engineering techniques, such as defined requirements, adequate documentation, quality assurance, and senior management approvals, before moving to the next stage of the life cycle. The SELC has seven stages: initiation and authorization, project definition, system design, construction, acceptance and readiness, operations, and retirement.

ii. Technology and Methodology

ATS-P processes traveler information against other information available to ATS, and applies risk-based rules based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence from DHS and other government agencies, to assist CBP officers in identifying individuals who require additional inspection or in determining whether individuals should be allowed or denied entry into the United States. The risk-based rules are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. Unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares information in ATS source databases against watch lists, criminal records, warrants, and patterns of suspicious activity identified through past investigations and intelligence. The results of these comparisons are either assessments of the risk-based rules that a traveler has matched or matches against watch lists, criminal records, or warrants. The rules are run against continuously updated incoming information about travelers (e.g., information in passenger and crew manifests) from the data sources listed below. While the rules are initially created based on information derived from past investigations and intelligence, data mining queries of data in ATS and its source databases may subsequently be used by analysts to refine or further focus those rules to improve the effectiveness of their application.

The results of queries in ATS-P are designed to signal to CBP officers that further inspection of a person may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise noted as a person of concern to law enforcement. The risk assessment analysis is generally performed in advance of a traveler's arrival in or departure from the United States, and becomes another tool available to DHS officers in determining admissibility and in identifying illegal activity. In lieu of more extensive manual reviews of traveler information and intensive interviews with every traveler arriving in or departing from the United States, ATS-P allows CBP personnel to focus their efforts on potentially high-risk passengers. CBP uses ATS-P for decision support and does not make decisions about individuals solely based on the results of the data mining of information in ATS-P. Rather, the CBP officer uses the information in ATS-P to assist in determining whether an individual should undergo additional inspection.

iii. Data Sources

ATS-P uses available information from the following databases to assist in the development of the risk-based rules discussed above. ATS-P vetting relies upon information in APIS; NIIS, which contains all Form I-94 Notice of Arrival/Departure records and actual ESTA arrivals/departures; ESTA, which contains pre-arrival information for persons traveling from Visa Waiver Program (VWP)[57] countries; the DHS Suspect and Violator Indices (SAVI); and the Department of State visa databases. ATS-P also relies upon PNR information from air carriers,

[57] The Visa Waiver Program allows eligible foreign nationals from participating countries to travel to the United States for business or pleasure, for stays of 90 days or less, without obtaining a visa. The Program requirements primarily are set forth in the Immigration and Nationality Act (INA), 8 U.S.C. § 1187, and 8 C.F.R. part 217. Section 711 of the 9/11 Commission Act amended Section 217 to strengthen the security of the VWP. ESTA is an outgrowth of that mandate. More information about ESTA is available at http://www.cbp.gov/esta.

BCI crossing data, seizure data, Report of International Transportation of Currency or Monetary Instrument Form (CMIR) data,[58] and information from the TSDB and TECS.

iv. Efficacy

ATS-P provides information to its users in near real-time. The flexibility of ATS-P's design and cross-referencing of databases permits CBP personnel to employ information collected through multiple systems within a secure information technology system, in order to detect individuals requiring additional scrutiny. The automated nature of ATS-P greatly increases the efficiency and effectiveness of the officers' otherwise manual and labor-intensive work checking separate databases, thereby facilitating the more efficient movement of travelers while safeguarding the border and the security of the United States. CBP officers use the information generated by ATS-P to aid their decision-making about the risk associated with individuals. As discussed below, ATS includes real-time updates of information from ATS source systems to ensure that CBP officers are acting upon accurate information.

In the past year, ATS-P has identified, through lookouts and/or risk-based rule sets, individuals who were confirmed matches to the TSDB and caused action to be taken to subject them to further inspection or, in some cases, took action to prevent them from boarding. ATS-P matches have also enabled CBP officers and foreign law enforcement partners to disrupt and apprehend persons engaged in human trafficking and drug smuggling operations. For example, CBP officers employed information in ATS-P, in conjunction with advance traveler data, to select a traveler arriving at Dallas, Texas for examination due to linkages to others arrested for narcotics smuggling. An inspection of the traveler's suitcase revealed 7.26 pounds of heroin. In another instance, ATS-P was used to review travel information for a traveler scheduled to fly to Japan from Los Angeles. During an inspection of the traveler's luggage, significant quantities of methamphetamine were discovered within jars of instant coffee and within the luggage hand rail. Finally, a traveler departing Amsterdam and intending to travel to Boston was referred to Immigration Advisory Program (IAP) personnel by officers using ATS-P to assess the traveler's risk.[59] A review of the traveler's document revealed residue where a visa had been present. IAP personnel turned over the traveler to Dutch officials, who confiscated the passport and charged the traveler with presenting an altered document.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.[60] As part of this inspection and examination process, each traveler seeking to enter the United States must first establish his or her identity, nationality, and, when appropriate, admissibility to the satisfaction of the CBP officer and then submit to inspection for

[58] The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.
[59] CBP IAP personnel are posted at the host country's airport are during processing of flights bound for the United States. These unarmed, plain clothes officers assist airline and security employees with review of traveler information during the processing of U.S.-bound flights to identify potential threats. See Immigration Advisory Program Fact Sheet available at: http://www.cbp.gov/linkhandler/cgov/travel/inspections_carriers_facilities/immig_advisor_program/immig_advis_prog.ctt/immig_advis_prog.pdf.
[60] *See, e.g.*, 19 U.S.C. §§ 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; 8 U.S.C. §§ 1221, 1357; 46 U.S.C. § 46501; and 49 U.S.C. § 44909.

customs purposes. The information collected is authorized pursuant to the EBSVERA,[61] ATSA, IRTPA, the INA, and the Tariff Act of 1930, as amended.[62] Much of the information collected in advance of arrival or departure can be found on routine travel documents that passengers and crew members may be required to present to a CBP officer upon arrival in or departure from the United States.

c) ATS-Land Module (ATS-L)

i. Program Description

ATS-L provides CBP Officers and Border Patrol Agents at the land border ports of entry Border Patrol locations with access to real-time databases to assess the risk posed by vehicles and their occupants, as well as pedestrians, as they cross the border. The module employs data obtained from CBP license plate readers and traveler documents to compare information against state DMV databases and datasets available through ATS to assess risk and to determine if a vehicle or its passengers may warrant further scrutiny. This analysis permits the officer or agent to prepare for the arrival of the vehicle at initial inspection and to assist in determining which vehicles might warrant referral for further evaluation. ATS-L's real-time assessment capability improves security at the land border while expediting legitimate travelers through the border crossing process.

ii. Technology and Methodology

ATS-L processes vehicle, vehicle occupant, and pedestrian information against other data available to ATS, and applies rules developed by subject matter experts (officers and agents drawing upon years of experience reviewing historical trends and current threat assessments), system learning rules (rules resulting from the system's weighting positive and negative results from subject matter expert rules), or affiliate rules (derived from data establishing an association with a known violator). System learning rules in ATS-L seek to identify high-risk vehicles by examining historical trends of CBP narcotics seizure record data from the land ports of entry. These rules are driven by algorithms to identify obvious and non-obvious relationships among data inputs (i.e., reviewing historical seizure data and applying trend analysis to incoming vehicle and traveler data). The system learning rules are being updated through the use of a new predictive model to help identify personal vehicles with an increased risk of transporting certain types of illegal drugs; they are being rolled out to ports of entry on a staggered basis.[63] The subject matter expert rules, which are designed by CBP personnel to create scenarios based upon officer experience and law enforcement or intelligence information, are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. ATS-L also compares license plate and DMV data to information in ATS source databases including watch lists, criminal records, warrants, and a statistical analysis of

[61] Pub. L. No. 107-173.
[62] 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.
[63] Although some variant of system learning rules has been in place since the advent of the ATS-L module, CBP's Office of Information Technology is conducting a pilot of a new vendor's product at certain ports along the Southwest Border; if successful, this product may replace or enhance the existing System Learning Rules algorithms. The pilot remains in the evaluation phase.

past crossing activity. The results of these comparisons are either assessments recommending further official interest in a vehicle and its occupants or supporting information for the clearance and admission of the vehicle and its occupants.

The results of positive queries in ATS-L are designed to signal to DHS officers that further inspection of a vehicle or its occupants may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise noted as a person of concern to law enforcement. The risk assessment analysis at the border is intended to permit a recommendation prior to the vehicle's arrival at the point of initial inspection, and becomes one more tool available to DHS officers in determining admissibility and in identifying illegal activity. In lieu of more extensive manual reviews of a person's information and intensive interviews with each occupant of a vehicle or pedestrian arriving in the United States, ATS-L allows DHS personnel to focus their efforts on potentially high-risk vehicles and occupants. DHS does not make decisions about individuals based solely on the information in ATS-L. Rather, the DHS officer uses the information in ATS-L to assist in determining whether an individual should undergo additional inspection.

iii. Data Sources

ATS-L uses available information from the following databases to assist in the development of the risk-based rules discussed above. ATS-L relies upon information in NIIS, ESTA, SAVI, and the DoS visa databases. ATS-L also relies upon TECS crossing data, seizure data, feeds from Nlets (formerly the National Law Enforcement Telecommunications System), NCIC, SEVIS, and information from the TSDB.

iv. Efficacy

ATS-L provides information to its users in real time, permitting an officer to assess his or her response to the crossing vehicle or pedestrian prior to initiating the border crossing process. The automated nature of ATS-L is a significant benefit to officer safety by alerting officers of potential threats prior to the vehicle's arrival at the point of inspection. It also greatly increases the efficiency and effectiveness of the officer's otherwise manual and labor-intensive work checking individual databases, thereby facilitating the more efficient movement of vehicles, their occupants, and pedestrians, while safeguarding the border and the security of the United States. CBP officers use the information generated by ATS-L to aid their decision-making about risk associated with vehicles, their occupants, and pedestrians. As discussed above, ATS includes real-time updates of information from ATS source systems to ensure that CBP officers are acting upon accurate information.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information about vehicles and their occupants prior to entering the United States.[64] As part of this inspection and examination process, the occupants of each vehicle seeking to enter the United States must first establish their identity, nationality, and, when appropriate, admissibility to the satisfaction of the CBP officer and must

[64] *See, e.g.*, 19 U.S.C. §§ 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; 8 U.S.C. §§ 1221, 1357; 22 U.S.C. § 401; 46 U.S.C. § 46501; and 49 U.S.C. § 44909.

submit to inspection for customs purposes. Information collection in ATS-L is pursuant to the authorities for information collection in ATS-P (i.e., EBSVERA;[65] ATSA; IRTPA; the INA, and the Tariff Act of 1930, as amended). Much of the information collected in advance of or at the time of arrival can be found on routine travel documents possessed by the occupants (which they may be required to present to a CBP officer upon arrival in the United States), the vehicle's license plate, and official records pertaining to the registry of the vehicle.

4. ATS Privacy Impacts and Privacy Protections

The DHS Privacy Office has worked closely with CBP to ensure that ATS satisfies the privacy compliance requirements for operation. As noted above, CBP completed an updated PIA and SORN for ATS in June 2012. CBP, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel conduct joint quarterly reviews of the risk-based targeting rules used in ATS to ensure that the rules are appropriate, relevant, and effective and assess whether privacy and civil liberties protections are adequate and consistently implemented.

Authorized CBP officers and personnel from ICE, TSA, and U.S. Citizenship and Immigration Services (USCIS) who are located at seaports, airports, land border ports, and operational centers around the world use ATS to support targeting-, inspection-, and enforcement-related requirements.[66] ATS supports, but does not replace, the decision-making responsibility of CBP officers and analysts. Decisions made or actions taken regarding individuals are not based solely upon the results of automated searches of data in the ATS system. Information obtained in such searches assists CBP officers and analysts in either refining their analysis or formulating queries to obtain additional information upon which to base decisions or actions regarding individuals crossing U.S. borders.

ATS relies upon its source systems to ensure the accuracy and completeness of the data they provide to ATS. When a CBP officer identifies any discrepancy regarding the data, the officer will take action to correct that information, when appropriate. ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real time, or near-real time, from TECS, which includes data accessed from NCIC and Nlets, as well as from ACE, AMS, ACS, AES, ESTA, NIIS, BCI, SEVIS, and APIS. When corrections are made to data in source systems, ATS updates this information in near-real time and uses only the latest data. In this way, ATS integrates all updated data (including accuracy updates) in as close to real time as possible.[67]

In the event that PII (such as certain data within a PNR) used by or maintained in ATS-P is believed by the data subject to be inaccurate, the subject has access to the redress process previously developed by DHS. The individual is provided information about this process during examination at secondary inspection. CBP officers have a brochure available to each individual entering and departing the United States that provides CBP's Pledge to Travelers. This pledge

[65] Pub. L. No. 107-173.

[66] TSA, ICE, USCIS, and personnel from the DHS Office of Intelligence and Analysis (I&A) have access only to a limited version of ATS. I&A personnel use ATS results in support of their authorized intelligence activities in accordance with applicable law, Executive Orders, and policy.

[67] To the extent information that is obtained from another government source is determined to be inaccurate, this problem would be communicated to the appropriate government source for remedial action.

gives each traveler an opportunity to speak with a passenger service representative to answer any questions about CBP procedures, requirements, policies, or complaints.[68] CBP has created the CBP INFO Center in its Office of Public Affairs to serve as a clearinghouse for all redress requests, which come to CBP directly and concern inaccurate information collected or maintained by its electronic systems, including ATS. This process is available even though ATS does not form the sole basis for identifying enforcement targets. To facilitate the redress process, DHS has created a comprehensive, Department-wide program, the Traveler Redress Inquiry Program (DHS TRIP), to receive all traveler-related comments, complaints, and redress requests affecting its component agencies. Through DHS TRIP, travelers can seek resolution regarding difficulties they experienced during their travel screening and inspection.[69]

Under the ATS PIA and SORN, and as a matter of DHS policy, CBP permits any subject of PNR or his or her representative to make administrative requests for access and amendment of the PNR. Procedures for individuals to access ATS information are outlined in the ATS SORN and PIA. These procedures mirror the procedures providing for access in the source systems for ingested data, so that individuals may gain access to their own data from either ATS or the source systems that provide input to ATS in accordance with the procedures set out in the SORN for each source system. The Freedom of Information Act (FOIA) provides an additional means of access to PII held in source systems.[70] Privacy Act and FOIA requests for access to information for which ATS is the source system are directed to CBP.[71]

ATS underwent the Security Authorization process in accordance with DHS and CBP policy and obtained its initial Security Authorization on June 16, 2006. ATS also completed a Security Risk Assessment on March 28, 2006, in compliance with FISMA, OMB policy, and National Institute of Standards and Technology guidance. The ATS Security Authorization and Security Risk Assessment were subsequently updated and are valid until January 21, 2014; a new Security Authorization is currently being developed.

Access to ATS is audited to ensure that only appropriate individuals have access to the system. CBP's Office of Internal Affairs also conducts periodic reviews of ATS to ensure that the system is being accessed and used only in accordance with documented DHS and CBP policies. Access to the data used in ATS is restricted to persons with a clearance approved by CBP, approved access to the separate local area network, and an approved password. All CBP process owners and all system users are required to complete annual training in privacy awareness and must pass an examination. If an individual does not take training, that individual loses access to all computer systems, including ATS. As a condition precedent to obtaining access to ATS, CBP employees are required to meet all privacy and security training requirements necessary to obtain access to TECS.

[68] The Pledge is available at http://www.cbp.gov/xp/cgov/travel/customerservice/pledge_travel.xml. In addition, travelers can visit CBP's INFO Center website at http://www.cbp.gov/xp/cgov/travel/customerservice/ to request answers to questions and submit complaints electronically. This website also provides travelers with the address of the CBP INFO Center and the telephone number of the Joint Intake Center.

[69] DHS TRIP can be accessed at: http://www.tsa.gov/traveler-information/dhs-traveler-redress-inquiry-program-dhs-trip.

[70] 5 U.S.C. § 552.

[71] Requests may be submitted by mail to FOIA Division, 799 9th Street NW, Mint Annex, Washington, DC 20229-1177, by email to CBPFOIA@dhs.gov.

As discussed above, ATS collects information directly and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems.

The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be disposed of in accordance with ATS's National Archives and Records Administration (NARA)-approved record retention schedule, except as noted below.[72] The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions and masking requirements: ATS-P users with PNR access will have access to PNR in an active database for up to five years, with the PNR depersonalized and masked after the first six months of this period. After the initial five-year retention period in the active database, the PNR will be transferred to a dormant database for a period of up to ten years. PNR in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be unmasked in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk.[73]

Information maintained only in ATS that is linked to law enforcement lookout records, and CBP matches to enforcement activities, investigations, or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

B. Analytical Framework for Intelligence (AFI)

1. 2013 Program Update

The 2012 Data Mining Report described AFI,[74] which was developed to augment DHS analysts' ability to review the data in ATS source systems and improve the risk-based rules used by ATS to identify individuals who may pose a heightened security risk.[75]

In 2013, AFI became the user interface for ICE's Intelligence Fusion System (IFS), which includes several ICE databases, as discussed in section IV.B.4 below. As a result, AFI now provides federated access to IFS for ICE analysts with active accounts in IFS. AFI also initiated the Cross Domain Capabilities (CDC) program pilot to enable analysts to view secret and SBU data on the same screens. Previously, all DHS data sources utilized in AFI had been unclassified. Under the CDC Pilot, user login information is collected as part of a cross domain guard[76] audit function to ensure security and information handling procedures. PII from AFI

[72] NARA approved the record retention schedule for ATS on April 12, 2008.
[73] These masking requirements have been implemented pursuant to the U.S.-European Union PNR Agreement entered into force on June 1, 2012. The Agreement is available on the Privacy Office website at http://www.dhs.gov/privacy-foia-reports#5.
[74] 2012 Data Mining Report at p. 17.
[75] The PIA for AFI is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf. The AFI SORN is available at http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm and in the Federal Register at 77 FR 33753 (June 7, 2012).
[76] A guard protects the integrity of each system, enabling the movement of unclassified information to a classified system.

will be transmitted through the guard from SBU to secret domains. The guard neither stores, generates, nor retains PII. The CDC Pilot allows more effective information flow between security domains, but does not allow the collection, retention or storage of any data other than user access information.

The CDC pilot, and the addition of IFS to AFI, will be included in a PIA update for AFI to be completed after the Privacy Office's PCR of AFI, which was underway as the reporting period for this report ended.

2. Program Description

AFI enhances CBP's ability to identify and apprehend individuals who pose a potential law enforcement or security risk, and aids in the enforcement and prosecution of customs and immigration laws, and other laws enforced by CBP at the border. AFI is used for the purposes of: (1) identifying individuals, associations, or relationships that may pose a potential law enforcement or security risk, targeting cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law; (2) conducting additional research on persons or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and (3) sharing finished intelligence products[77] developed in connection with the above purposes with DHS employees who have a need to know in the performance of their official duties and who have appropriate clearances or permissions, or externally pursuant to routine uses in the AFI SORN.

AFI augments CBP's ability to gather and develop information about persons, events, and cargo of interest by creating an index of the relevant data in the existing operational systems and providing AFI analysts with different tools that assist in identifying non-obvious relationships. AFI allows analysts to generate finished intelligence products to better inform finished intelligence product users about why an individual or cargo may be of greater security interest based on the targeting and derogatory information identified in or through CBP's existing data systems. CBP currently utilizes transaction-based systems such as TECS and ATS for targeting and inspections. AFI enhances the information from those systems by utilizing different analytical capabilities and tools that provide link analysis among data elements as well as the ability to detect trends, patterns, and emerging threats.

AFI improves the efficiency and effectiveness of CBP's research and analysis process by providing a platform for the research, collaboration, approval, and publication of finished intelligence products. AFI analysts use AFI to conduct research on individuals, cargo, or conveyances to understand whether there are patterns that could assist in the identification of potential law enforcement or security risks.

AFI provides a set of analytic tools that include advanced search capabilities into existing DHS sources, and federated queries to other federal agency sources and commercial data aggregators, to allow analysts to search several databases simultaneously. AFI tools scan the query results,

[77] "Finished Intelligence Products" are tactical, operational, and strategic law enforcement intelligence products that have been reviewed and approved for sharing with finished intelligence product users and authorities outside DHS.

associate and extract similar themes, and present the results to the AFI analyst in a manner that allows for easy visualization and analysis.

AFI creates an index of the relevant data in existing operational DHS source systems by ingesting this data from source data systems, as described below. AFI also permits AFI analysts to upload, index, and store information that may be relevant from other sources, such as the Internet or traditional news media, subject to the procedures described below. Requests for Information (RFI), responses to RFIs, finished intelligence products, and unfinished "projects"[78] are also part of the index. The indexing engines refresh data from the originating system periodically depending on the source data system. AFI adheres to the records retention policies of the source data systems along with their user access controls.

The AFI index permits AFI analysts to perform faster and more thorough searches because the indexed data allows for a search across all identifiable information in a record, including free-form text fields and other data that might not be searchable through the source system. Within AFI, this is a quick search that shows where a particular individual or characteristic arises. With other systems, a similar search for a particular individual requires several queries across multiple systems to retrieve a corresponding response and may not contain all relevant instances of the search terms.

AFI also enables analysts to perform federated queries against external data sources, including certain data sets belonging to the Department of State, DOJ/FBI, and commercial data aggregators that are already available to DHS users. AFI tracks where AFI analysts search and routinely audits these records. AFI analysts use data that is available from commercial data aggregators to complement or clarify the data to which they have access within DHS. AFI provides a suite of tools that assist analysts in detecting trends, patterns, and emerging threats, and in identifying non-obvious relationships, using the information maintained in the index and made accessible through the federated query.

AFI also serves as a workspace that allows AFI analysts to create finished intelligence products, to maintain and track projects throughout their lifecycle from inception to finished intelligence product or from RFI to response, and to share finished intelligence products either within DHS or externally through regular law enforcement and intelligence channels to authorized users with a need to know, pursuant to routine uses in the AFI SORN.[79]

3. Technology and Methodology

AFI creates and retains an index of searchable data elements in existing operational DHS source systems by ingesting this data through and from its source systems. The index indicates which source system records match the search term used. AFI maintains the index of the key data elements that are personally identifiable in source data systems. The indexing engines refresh data from the source system periodically. Any changes to source system records, or the addition or deletion of source system records, will be reflected in corresponding amendments to the AFI index as the index is routinely updated.

[78] AFI analysts create "projects" within the AFI workspace to capture research and analysis that is in progress and may or may not lead to a finished intelligence product or RFI response.
[79] A detailed description of the processes leading to finished intelligence products and RFI responses is included in the PIA for AFI.

AFI includes a suite of tools designed to give AFI analysts visualization, modeling, collaboration, analysis, summarization, and reporting capabilities. These include text analysis, link analysis (social network analysis), statistical analysis, and geospatial analysis.

Specific types of analysis include:

- *Statistical analysis*: Statistical analysis provides modeling and statistical tools that can help analysts discover patterns or generalizations in the data. This analysis can produce models that can be used to identify similar patterns in other data or common characteristics among seemingly disparate data.
- *Geospatial analysis*: Geospatial analysis utilizes visualization tools to display a set of events or activities on a map showing streets, buildings, geopolitical borders, or terrain. This analysis can help produce intelligence about the location or type of location that is favorable for a particular activity.
- *Link analysis*: Link analysis provides visualization tools that can help analysts discover patterns of associations among various entities. This analysis can produce a social network representation of the data.
- *Temporal analysis*: Temporal analysis offers visualization tools that can display events or activities in a timeline to help an analyst identify patterns or associations in the data. This analysis can produce a time sequence of events that can be used to predict future activities or discover other similar types of activities.

The results of these analyses are used to generate finished intelligence products, responses to RFIs, and projects. The finished intelligence products are published in AFI for finished intelligence product users to search. Several forms of the analyses involve aspects of data mining; both the statistical and link analyses employ characteristics of behavior, associations, or circumstances to identify patterns of activity or networks. In all situations, research developed or reports created by AFI analysts are subject to supervisory review to confirm a rational relationship between the subject of a query and the responsive information. This review also extends to the scope and context of the responsive information to ensure that a compiled report remains germane to its initial purpose. Further consideration is given to the intended audience of a product or report. AFI does not permit dissemination within its user community of products or reports that lack supervisory approval. No decisions about individuals are made exclusively on the basis of the results of research obtained from AFI.

4. Data Sources

The AFI system does not itself collect information directly from individuals. Rather, AFI performs searches for and accesses information collected and maintained in other systems, including information from both government-owned sources and commercial data aggregators. Additionally, AFI analysts may upload information that they determine is relevant to a project, including information publicly available on the Internet. .

AFI uses, disseminates, or maintains seven categories of data containing PII:

- *DHS-Owned Data that AFI automatically collects and stores*: This data is indexed and then as information is retrieved via a search, data from multiple sources may be joined to create a more complete representation of an event or concept. For example, a complex

event such as a seizure that is represented by multiple records may be composed into a single object for display. AFI receives records through:

- ATS (including: APIS; ESTA; TECS Incident Report Logs and Search, Arrest, Seizure Reports, Primary Name Query, Primary Vehicle Query, Secondary Referrals, TECS Intel Documents; and visa data);
- Enterprise Management Information System-Enterprise Data Warehouse (including: Arrival and Departure Form I-94; CMIR data; apprehension, inadmissibility, and seizure information from the ICE Immigration and Enforcement Operational Records System (ENFORCE); National Security Entry-Exit Program information from ENFORCE; SEVIS information; and seizure information from the Seized Asset and Case Tracking System);
- the Targeting Framework (case information).

- *DHS-Owned Data to which AFI provides federated access*: This data is a limited set of data owned, stored, and indexed by other DHS components. Through AFI, only a user with an active account in that other DHS system can query and receive results from that system. AFI will store only results that are returned as a function of AFI's audit capabilities. AFI provides this federated access to IFS. IFS includes the following information: Enforcement Integrated Database detention data, ICE intelligence information reports, ICE intelligence products, ICE name trace, ICE significant event notification Detention and Removal Leads, and TECS Reports of Investigation).[80]
- *Other Government Agency Data*: AFI obtains imagery data from the National Geospatial-Intelligence Agency and obtains other government agency data to the extent available through ATS, such as identity and biographical information, wants and warrants, DMV data, and data from the TSDB.[81]
- *Commercial Data*: AFI collects identity and imagery data from several commercial data aggregators so that DHS AFI analysts can cross-reference that information with the information contained in DHS-owned systems. Commercial data aggregators include sources available by subscription only (e.g., Thomson Reuters CLEAR) that connect directly to AFI, and do not include information publicly available on the Internet.
- *AFI Analyst-Provided Information*: This includes any information uploaded by an authorized user either as original content or from an *ad hoc* data source such as the Internet or traditional news media. AFI analyst-provided information may include textual data (such as official reports users have seen as part of their duties or segments of a news article), video and audio clips, pictures, or any other information the user determines is relevant. User-submitted RFIs and projects are also stored within AFI, as well as the responses to those requests.

[80] ICE and the Privacy Office issued a PIA for IFS on November 17, 2008. The IFS PIA is available at http://www.dhs.gov/privacy/xlibrary/assets/privacy/privacy_pia_ice_ifs.pdf.
[81] A more complete discussion of other government agency data that may be accessed through ATS can be found in the ATS PIA.

- *AFI Analyst-Created Information*: AFI maintains user-created projects as well as finished intelligence products. Finished intelligence products are made available through AFI to finished intelligence users.
- *Index Information*: As noted above, AFI ingests subsets of data from CBP and DHS systems to create an index of searchable data elements. The index indicates which source system records match the search term used.

The data elements that may be maintained in these seven categories include: full name, date of birth, gender, travel information, passport information, country of birth, physical characteristics, familial and other contact information, importation/exportation information, and enforcement records.

5. Efficacy

AFI became operational in August 2012. CBP has since sought to deploy AFI to field and headquarters locations to assign officers, agents, and employees user roles and to provide training commensurate with those roles. Initial testing and operational use of AFI along the Southwest border have shown that AFI provides valuable assistance to ongoing operations. For example, a user from the California Corridor Campaign received an unclassified Intel Alert notification from AFI based on the alerts the individual was monitoring. The analysis showed that the alert mentioned that the user's area of responsibility was being utilized to smuggle narcotics. The Intel Alert was distributed through chain of command and specific targeting was initiated by the Cargo Analysis Research Investigative Team unit. Seven days later, the Calexico port-of-entry commercial facility interdicted and seized 1265.86 kilograms of marijuana.

In another instance, an AFI user analyzed narcotics and weapon seizures, alien apprehensions, and assaults on CBP personnel while on duty to determine how best to allocate resources. The user analyzed the locations and times when the highest rates of seizures occurred with the lowest rates of assaults on CBP personnel. The information from this analysis was imported into AFI's analytical tool and exported into geospatial and temporal graphs. This work resulted in a significant increase in arrests and disrupts.

6. Laws and Regulations

Numerous authorities mandate that DHS and CBP provide border security and safeguard the homeland, including: Title II of the Homeland Security Act (Pub. L. 107-296), as amended by IRTPA; the Tariff Act of 1930, as amended; the INA (8 U.S.C. § 1101, et seq.); the 9/11 Commission Act (Pub. L. 110-53); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132); the SAFE Port Act; ATSA; and 6 U.S.C. § 202.

7. Privacy Impact and Privacy Protections

CBP does not use the information in AFI to make unevaluated automated decisions about individuals. Given the breadth of the data available to AFI users, CBP has built extensive privacy protections into the structure and governance of AFI.[82] AFI does not collect information

[82] The PIA for AFI includes a more complete description of these protections.

directly from individuals; AFI source systems are responsible, as appropriate, for providing individuals an opportunity to decline to provide information or to consent to or opt out of use information. AFI provides the public notice about its use of information through its PIA and SORN.

The CDC does not allow the collection, retention, or storage of any data except for user access information. Additionally, it audits all cross-domain transfers to ensure that all information is handled properly and all security procedures have been followed.

AFI is being designed and developed in an iterative, incremental fashion. CBP has created a governance board to ensure that AFI is built and used in a manner consistent with the Department's authorities and that information in AFI is used consistent with the purpose for which it was originally collected. The governance board includes representatives from CBP's Offices of Intelligence and Investigative Liaison, Field Operations, Border Patrol, Air & Marine, Chief Counsel, Internal Affairs, Information Technology, and Privacy and Diversity, who review requested changes to the system on a quarterly basis and determine whether additional input is required. The governance board directs the development of new aspects of AFI, and reviews and approves new or changed uses of AFI, new or updated user types, and new or expanded data to be made available in or through AFI. As an added layer of oversight, the DHS Privacy Office initiated a PCR for AFI in August 2013, and the PCR was underway as the reporting period for this report ended.

Although AFI indexes information from many different source data systems, each source system maintains control of the data that it originally collected, even though the data is co-located in both the source system and in AFI. Accordingly, only DHS AFI analysts authorized to access the data in a particular source system have access to that same data through AFI.[83] This is accomplished by passing individual user credentials from the originating system or through a previously approved certification process in another system. Finished intelligence product users and DHS AFI analysts have access to finished intelligence products, but only DHS AFI analysts have access to the source data, projects, and analytical tools maintained in AFI. In order to access AFI, all AFI users are required to complete biannual training in privacy awareness and the privacy training required of all CBP employees with access to CBP's law enforcement systems. This training is regularly updated. Users who do not complete this training lose access to all computer systems, including AFI.

As AFI does not collect information directly from the public or any other primary source, it depends on the system(s) performing the original collection to ensure data accuracy. DHS AFI analysts will use a variety of data sources available through the source systems to verify and correlate the available information to the greatest extent possible. The accuracy of DHS-owned data, other federal agency data, and data provided by commercial data aggregators is dependent on the original source. DHS AFI analysts are required to make changes to the data records in the underlying DHS system of record if they identify inaccurate data and alert the source agency of the inaccuracy; AFI will then reflect the corrected information. Additionally, as the source systems for other federal agency data or commercial data aggregators correct information, queries of those systems will reflect the corrected information.

[83] Only authorized CBP personnel and analysts who require access to the functionality and data in AFI as a part of the performance of their official duties and who have appropriate clearances or permissions will have access to AFI.

In order to further mitigate the risk of AFI's retaining incorrect, inaccurate, or untimely information, AFI routinely updates its index to ensure that only the most current data are available to its users. Any changes to source system records, or the addition or deletion of a source system record, is reflected in the corresponding amendments to the AFI index when the index is updated. Further, when a user accesses individual records, the records are retrieved directly from the source system to ensure data quality. AFI also requires that users recertify annually any user-provided information marked as containing PII to ensure its continued relevance and accuracy. If the information is not recertified, it is automatically purged from the system.

AFI has built-in system controls that identify what particular users are able to view, query, or write, as well as audit functions that are routinely reviewed. AFI uses security and auditing tools to ensure that information is used in accordance with CBP policies and procedures. The security and auditing tools include: *Role-Based Access Control*, which determines a user's authorization to use different functions, capabilities, and classifications of data within AFI, and *Discretionary Access Control*, which determines a user's authorization to access individual groupings of user-provided data. Data are labeled and restricted based on data handling designations for SBU data (e.g., FOUO, SSI, Law Enforcement Sensitive (LES)) and based on need to know.

AFI has been developed to meet Intelligence Community standards to prevent unauthorized access to data, ensuring that isolation between users and data is maintained based on need-to-know. Application logging and auditing tools monitor data access and usage, as required by the information assurance policies against which AFI was designed, developed, and tested (including DHS Management Directive 4300 A/B). AFI completed its most recent Security Authorization on April 12, 2013, and was granted a three-year authority to operate (ATO) from the DHS Office of the Chief Information Security Officer. The government systems accessed or used by AFI have undergone Security Authorization and are covered by their respective ATOs.

As AFI contains sensitive information related to intelligence, counterterrorism, homeland security, and law enforcement programs, activities, and investigations, DHS has exempted AFI from the access and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(j)(2) and (k)(2). For index data and source data, as described in the SORN for AFI, to the extent that a record is exempted in a source system, the exemption will continue to apply. When there is no exemption for giving access to a record in a source system, CBP will provide access to that information maintained in AFI.[84]

AFI adheres to the records retention policies of its source data systems. AFI is in the process of completing NARA requirements for data retention to obtain a records schedule. AFI is proposing that projects be retained for up to 30 years, RFIs and responses to RFIs for 10 years, and finished intelligence products for 20 years. These retention periods would be commensurate with those in place for similar records in DHS.

[84] Notwithstanding the applicable exemptions, CBP reviews all requests for access to records in AFI on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP, and in accordance with procedures published in the applicable SORN. Requests may be submitted to U.S. Customs and Border Protection, Freedom of Information Act (FOIA) Division, Mint Annex Building, 1300 Pennsylvania Avenue, NW, Washington, DC 20229. Additional information on submitting FOIA and Privacy Act requests is included in the PIA for AFI at pp. 22-23.

C. FALCON Data Analysis and Research for Trade Transparency System (FALCON-DARTTS)

1. 2013 Program Update

Shortly after the reporting period for this report ended, ICE migrated the DARTTS system to the ICE Homeland Security Investigations (HSI) FALCON environment and launched FALCON-DARTTS. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other government applications and systems, with appropriate user access restrictions and robust user auditing controls.[85] FALCON-DARTTS replicates the functionality of and serves the same user-groups as legacy DARTTS. With the deployment of FALCON-DARTTS, the legacy DARTTS system was retired.[86]

On January 16, 2014, ICE published a new PIA for FALCON-DARTTS to address the migration from legacy DARTTS and capture several new system features, including: (1) additional datasets and records, (2) enhanced user access controls that allow only datasets authorized for a user-specific profile to be visible and accessible by that user, (3) an updated way in which datasets are physically separated, and (4) new interaction with FALCON Search & Analysis (FALCON-SA).[87]

In addition to the trade, financial, and law enforcement datasets discussed in the 2012 DHS Data Mining Report, ICE has added to FALCON-DARTTS financial data provided by other federal, state, and local law enforcement agencies. Other financial data consists of U.S. and foreign financial data that has been obtained via official investigations, legal processes, and/or legal settlements. ICE has also added records manually uploaded into FALCON-DARTTS on an *ad hoc* basis by authorized ICE FALCON-DARTTS users, which may be obtained from various sources, such as financial institutions, transportation companies, manufacturers, customs brokers, state, local, and foreign governments, free trade zones, and port authorities, and may include financial records, business records, trade transaction records, and transportation records.

As was true for the legacy DARTTS system, ICE HSI personnel, select CBP personnel, and foreign government partners are granted access to analyzed FALCON-DARTTS data. In FALCON-DARTTS, system access controls ensure that all ICE HSI, CBP, and foreign users are able to access only data that is associated with the user's specific profile and which that user has the legal authority to access. Specifically, only ICE HSI and CBP users are granted access to the law enforcement data, and only ICE HSI users are granted access to the financial data,

[85] In February 2012, ICE deployed the first module of FALCON with the launch of FALCON Search & Analysis (FALCON-SA). FALCON-SA provides the capability to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. For more information on the FALCON environment, *see* DHS/ICE/PIA-032A FALCON Search & Analysis System (FALCON-SA), January 16, 2014, http://www.dhs.gov/sites/default/files/publications/privacy_ice_flaconsa_january2014.pdf.

[86] The legacy DARTTS system is described in the DHS/ICE-PIA – 006 DARTTS PIA, October 20, 2008, and subsequent updates. *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_dartts.pdf.

[87] The PIA for FALCON-DARTTS (DHS/ICE/PIA-038) is available at http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falcondartts_January 2014_0.pdf.

maintained in FALCON's general data storage environment.[88] In this environment, the data is aggregated with other FALCON data, and user access is controlled through a combination of data tagging, access control lists, and other technologies. Some law enforcement data used in FALCON-DARTTS analyses is already stored in the FALCON general data storage environment; therefore it does not need to be replicated again for use by FALCON-DARTTS. Using a central data store for most FALCON data enhances privacy overall by eliminating the need for multiple copies of the same data.

The 2012 Data Mining Report discussed DARTTS World, a separate web-based instance of the legacy DARTTS system specifically dedicated for use by foreign government partners. DARTTS World was retired during the transition to FALCON-DARTTS. Foreign users of FALCON-DARTTS are authorized to access only trade data, and are not authorized to access the law enforcement, financial data, or *ad hoc* data that resides in the FALCON general data storage environment. The trade data is stored in a "trade data subsystem" that is physically and logically separate from the FALCON general data storage environment and contains different user access requirements than the overarching data storage environment. Trade data is segregated in a separate storage environment due to its high volume and to enhance security controls for foreign users who only access trade data. Access by FALCON-DARTTS users to the trade data stored in this subsystem occurs through one of two web applications: (1) ICE HSI and CBP users are granted access to all U.S. and foreign trade data via an internal DHS FALCON-DARTTS web application that resides within the DHS/ICE network, and (2) foreign users are granted access to select trade datasets via a different web application that resides within a protected infrastructure space between the DHS Internet perimeter and the DHS/ICE network. Foreign users are able to access only the trade data related to their country and the related U.S. trade transactions, unless access to other partner countries' data is authorized via information sharing agreements. Foreign users are able to use the analytical tools available in FALCON-DARTTS to analyze trade data, without creating a risk of unauthorized access to or use of financial or law enforcement data.

As FALCON-DARTTS is a component of the larger FALCON environment, select datasets in FALCON-DARTTS are routinely ingested into and available in FALCON-SA for additional analysis and investigation using the tools available in FALCON-SA. These datasets include U.S. and foreign financial data[89] and the Specially Designated Nationals (SDN) List, a list of individuals and companies owned or controlled by, or acting on behalf of, targeted countries compiled and maintained by U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and made publicly available on the OFAC website.[90] The SDN List will be available to all FALCON-SA users for use in any investigation initiated in FALCON-SA. For financial data, however, only FALCON-SA users who are also granted FALCON-DARTTS privileges will be authorized to access the financial data via the FALCON-SA interface; other FALCON-SA users without FALCON-DARTTS privileges are unable to view, access, or analyze the FALCON-

[88] The FALCON general data storage environment consists of data ingested on a routine or *ad hoc* basis from other existing sources. The data stored in the general data storage environment is structured and optimized for use with the analytical tools in FALCON-SA and the other FALCON modules.

[89] Other datasets, such as TECS, that are already stored in FALCON's general data storage environment will also be used by FALCON-DARTTS users for analysis and investigation in FALCON-SA.

[90] *See* www.treasury.gov/ofac.

DARTTS financial data.[91] FALCON-SA enforces these access restrictions by requiring users to designate their projects within the system as Trade Transparency Unit (TTU) investigations; otherwise, the financial datasets will not be available for use and analysis in FALCON-SA.[92]

In addition, for trade data only, ICE HSI investigators may import on an *ad hoc* basis their analytical results from FALCON-DARTTS into FALCON-SA for additional analysis and investigation using the tools available in FALCON-SA. These trade results are tagged as "FALCON-DARTTS trade data" in FALCON-SA, and the user may publish the data in the system so that they are accessible by all FALCON-SA users who have also been granted FALCON-DARTTS privileges.[93]

Additional information about FALCON-DARTTS is included in an annex to this report that contains LES information and is being provided separately to Congress.

2. Program Description

ICE maintains FALCON-DARTTS, which generates leads for and otherwise supports investigations of trade-based money laundering, contraband smuggling, trade fraud, and other import-export crimes led by ICE HSI. FALCON-DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation. These anomalies are then independently confirmed and further investigated by experienced HSI investigators.

FALCON-DARTTS is owned and operated by the HSI TTU. Trade transparency is the concept of examining U.S. and foreign trade data to identify anomalies in patterns of trade. Such anomalies can indicate trade-based money laundering or other import-export crimes that HSI is responsible for investigating, such as smuggling, trafficking counterfeit merchandise, the fraudulent misclassification of merchandise, and the over- or under-valuation of merchandise to conceal the source of illicitly derived proceeds or as the means to earn illicitly derived funds supporting ongoing criminal activity. As part of the investigative process, HSI investigators and analysts must understand the relationships among importers, exporters, and the financing for a set of trade transactions, to determine which transactions are suspicious and warrant investigation. FALCON-DARTTS is designed specifically to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator.

FALCON-DARTTS allows HSI to perform research and analysis that are not possible in any other ICE system because of the data it analyzes and the level of detail at which the data can be analyzed.[94] FALCON-DARTTS does not seek to predict future behavior or "profile" individuals or entities (i.e., identify individuals or entities that meet a certain pattern of behavior pre-determined to be suspect). Instead, it identifies trade and financial transactions that are statistically anomalous based on user-specified queries. Investigators analyze the anomalous

[91] Access to, and use of, financial data is also subject to the U.S. Department of the Treasury's Financial Crimes Enforcement Network's *Revised Re-Dissemination Guidelines for Bank Secrecy Act Information* (November 28, 2007).
[92] ICE updated the FALCON-SA PIA Appendix to reflect that the SDN List and financial data are routinely ingested into FALCON-SA. See DHS/ICE/PIA-032A FALCON-SA.
[93] ICE updated the FALCON-SA PIA Appendix to reflect that trade results are imported on an *ad hoc* basis into FALCON-SA. See DHS/ICE/PIA-032A FALCON-SA.
[94] For example, FALCON-DARTTS allows investigators to view totals for merchandise imports and then sort on any number of variables, such as country of origin, importer name, manufacturer name, or total value.

transactions to determine if they are in fact suspicious and warrant further investigation. If determined to warrant further investigation, they will gather additional facts, verify the accuracy of the FALCON-DARTTS data, and use their judgment and experience in deciding whether to investigate further. Not all anomalies lead to formal investigations.

FALCON-DARTTS is used by HSI special agents and intelligence research specialists who work on TTU investigations at ICE Headquarters and in the ICE HSI field and foreign attaché offices, as well as properly cleared support personnel. In addition, select CBP personnel and foreign government partners have limited access to FALCON-DARTTS. CBP customs officers and import specialists who conduct trade transparency analyses in furtherance of CBP's mission use the trade and law enforcement datasets within FALCON-DARTTS to identify anomalous transactions that may indicate violations of U.S. trade laws. Foreign government partners that have established TTUs and have entered into a Customs Mutual Assistance Agreement (CMAA) or other similar information sharing agreement with the United States use specific trade datasets to investigate trade transactions, conduct analysis, and generate reports in FALCON-DARTTS. All ICE HSI, CBP, and foreign users of FALCON-DARTTS are able to access only data that is associated with the user's specific profile and which that user has the legal authority to access.

3. Technology and Methodology

FALCON-DARTTS uses COTS software to assist its users in identifying suspicious trade transactions by analyzing trade and financial data and identifying data that is statistically anomalous. In response to user-specified queries, the software application is designed to analyze structured and unstructured data using three tools: the drill-down technique,[95] link analysis, and charting and graphing tools that use proprietary statistical algorithms.[96] It also allows non-technical users with investigative experience to analyse large quantities of data and rapidly identify problem areas. The program makes it easier to apply their specific knowledge and expertise to complex sets of data.

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

FALCON-DARTTS can also identify links between individuals and/or entities based on commonalities, such as identification numbers, addresses, or other information. These

[95] The drill-down system allows HSI investigators to quickly find, analyze, share, and document suspicious patterns in large amounts of data, and to continually observe and analyze patterns in data at any point. HSI investigators can also connect one dataset within FALCON-DARTTS to another, to see whether the suspicious individuals, entities, or patterns occur elsewhere.

[96] FALCON-DARTTS provides HSI investigators the means to represent data graphically in graphs, charts, or tables to aid in the visual identification of anomalous transactions. FALCON-DARTTS does not create new records to be stored in FALCON-DARTTS.

commonalities in and of themselves are not suspicious, but in the context of additional information, they can assist investigators in identifying potentially criminal activity and lead to identification of witness, other suspects, or additional suspicious transactions.

FALCON-DARTTS uses trade data, financial data, and law enforcement data provided by other U.S. government agencies and foreign governments (hereafter referred to as "raw data") .[97] ICE receives data from the sources listed below via CD-ROM, external storage devices, or electronic data transfers and loads the data into FALCON-DARTTS and the FALCON general data storage environment. The agencies that provide FALCON-DARTTS with trade data collect any PII directly from individuals or enterprises completing import-export electronic or paper forms.[98] Agencies that provide FALCON-DARTTS with financial data receive PII from individuals and institutions, such as banks, that are required to complete certain financial reporting forms.[99] PII in the raw data is necessary to link related transactions together. It is also necessary to identify persons or entities that should be investigated further.

HSI investigators with experience conducting financial, money laundering, and trade fraud investigations use completed FALCON-DARTTS analyses to identify possible criminal activity and provide support to field investigations. Depending on their specific areas of responsibility, HSI investigators may use the analyses for one or more purposes. HSI investigators at ICE Headquarters refer the results of FALCON-DARTTS analyses to HSI field offices as part of an investigative referral package to initiate or support a criminal investigation. HSI investigators in domestic field offices can also independently generate leads and subsequent investigations using FALCON-DARTTS analyses. HSI investigators in HSI attaché offices at U.S. Embassies abroad use the analyses to respond to inquiries from foreign partner TTUs. If a foreign TTU identifies suspicious U.S. trade transactions of interest, HSI investigators will validate that the transactions are, in fact, suspicious, and ICE will coordinate joint investigations on those specific trade records. ICE may also open its own investigation into the matter.

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

Similarly, HSI investigators may access U.S. and foreign financial data from FALCON-DARTTS in FALCON-SA to conduct additional analysis and investigation using the tools and additional data available in FALCON-SA. These datasets are routinely ingested into FALCON-

[97] Foreign trade data may include: names of importers, exporters, and brokers; addresses of importers and exporters; Importer IDs; Exporter IDs; Broker IDs; and Manufacturer IDs.

[98] U.S. trade data includes the following PII: names and addresses (home or business) of importers, exporters, brokers, and consignees; Importer and Exporter IDs (e.g., an individual's or entity's Social Security or Tax Identification Number); Broker IDs; and Manufacturer IDs.

[99] Financial data includes the following PII: names of individuals engaging in financial transactions that are reportable under the Bank Secrecy Act (BSA), 31 U.S.C. §§ 5311-5332, (e.g., cash transactions over $10,000); addresses; Social Security/Taxpayer Identification Numbers; passport number and country of issuance; bank account numbers; party names and addresses; and owner names and addresses.

SA, and only FALCON-SA users who are also granted FALCON-DARTTS privileges will be authorized to access the financial data via the FALCON-SA interface.

4. Data Sources

All raw data analyzed by FALCON-DARTTS is provided by other U.S. agencies and foreign governments, and is divided into the following broad categories: U.S. trade data, foreign trade data, financial data, and law enforcement data. U.S. trade data is (1) import data in the form of an extract from ACS, 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 ACS; (2) EEI submitted to AES; and (3) bill of lading data collected by CBP via the AMS and provided to ICE through electronic data transfers for upload into FALCON-DARTTS.

Foreign import and export data in FALCON-DARTTS is provided to ICE by partner countries pursuant to a CMAA or other similar agreement. Certain countries provide trade data that has been stripped of PII. Other countries provide complete trade data, which includes any individuals' names and other identifying information that may be contained in the trade records.

ICE receives U.S. financial data from FinCEN and other federal, state, and local law enforcement agencies. FinCEN data is in the form of the following financial transaction reports: CMIRs (transportation of more than $10,000 into or out of the United States at one time); Currency Transaction Reports (deposits or withdrawals of more than $10,000 in currency into or from a domestic financial institution); Suspicious Activity Reports (information regarding suspicious financial transactions within depository institutions, money services businesses,[100] the securities and futures industry, and casinos and card clubs); Reports of Coins or Currency Received in a Non-Financial Trade or Business (transactions involving more than $10,000 received by such entities); and data provided in Reports of Foreign Bank and Financial Accounts (reports by U.S. persons who have financial interest in, or signature or other authority over, foreign financial accounts in excess of $10,000). Other financial data collected by other federal, state, and local law enforcement agencies is collected by such agencies in the course of an official investigation, through legal processes, and/or through legal settlements and has been provided to ICE to deter international money laundering and related unlawful activities.[101]

ICE receives law enforcement records from the SDN List and CBP's TECS system (subject records). In addition to listing individuals and companies owned or controlled by, or acting on behalf of, targeted countries, the SDN List includes information about foreign individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Their assets are blocked, and U.S. persons and entities are generally prohibited from dealing with them. FALCON-DARTTS analysis of the SDN List allows ICE

[100] Under 31 U.S.C. § 5318, a money services business (MSB) is required by the BSA to complete and submit Suspicious Activity Reports to FinCEN. Entities qualifying as MSBs are defined under 31 C.F.R. § 1010.100(ff).31 U.S.C. § 5318. They include money transmitters; issuers; redeemers and sellers of money orders and travelers' checks; and check cashers and currency exchangers. FinCEN administers the BSA, which requires financial depository institutions and other industries vulnerable to money laundering to take precautions against financial crime, including reporting financial transactions possibly indicative of money laundering. 31 U.S.C. §§ 5311-5330.
[101] For example, a court may direct a corporation to provide data to law enforcement agencies after determining that the corporation did not practice due diligence to deter money laundering and/or has facilitated criminal activities.

HSI users to rapidly determine whether international trade and/or financial transactions with a specially designated individual or entity are being conducted, thus providing ICE HSI with the ability to take appropriate actions in a timely and more efficient manner.

Subject records created by ICE HSI users from CBP's TECS database pertain to persons, vehicles, vessels, businesses, aircraft, etc. FALCON-DARTTS accesses this data stored within the FALCON general data storage environment, eliminating the need for an additional copy of the data. FALCON-DARTTS analysis of TECS subject records allows ICE HSI users to quickly determine if an entity that is being researched in FALCON-DARTTS is already part of a pending investigation or was involved in an investigation that is now closed.

In addition to the raw data collected from other agencies and foreign governments, ICE HSI users are permitted to manually upload records into FALCON-DARTTS on an *ad hoc* basis. Information uploaded on an *ad hoc* basis is obtained from various sources such as financial institutions, transportation companies, manufacturers, customs brokers, state, local, and foreign governments, free trade zones, and port authorities, and may include financial records, business records, trade transaction records, and transportation records. For example, pursuant to an administrative subpoena, HSI investigators may obtain financial records from a bank associated with a shipment of merchandise imported into a free trade zone. Both the ability to upload information on an *ad hoc* basis and to access *ad hoc* data is limited to ICE HSI FALCON-DARTTS users only.

FALCON-DARTTS itself is the source of analyses of the raw data produced using analytical tools within the system.

5. Efficacy

Prior to the migration to FALCON-DARTTS, the legacy DARTTS system had proven to be an effective tool for ICE HSI in identifying criminal activity during the reporting period. Through the use of legacy DARTTS, domestic HSI field offices and foreign attaché offices had the ability to initiate and enhance criminal cases related to trade-based money laundering and other financial crimes. Information derived from legacy DARTTS was essential in several criminal prosecutions and enforcement actions both domestically and abroad. For example, using information gathered through trade and financial queries in legacy DARTTS, HSI TTU assisted HSI Miami in an investigation involving a subject who was believed to be involved in an over/under-valuation scheme of gold imports. Further investigation revealed that the subject was involved in operating an unlicensed money service business and a possible Ponzi scheme. In May 2013, subjects were arrested for violations of 18 U.S.C. § 1349 (conspiracy to commit wire fraud). In June 2013, subjects were indicted for violations of 18 U.S.C. § 1343 (fraud by wire, radio, or television), 18 U.S.C. § 1349 (attempt and conspiracy), and 18 U.S.C. § 1956(h) (conspiracy to launder monetary instruments).

Legacy DARTTS was also used in support of enforcement actions. For example, as reported in the 2012 Report, HSI Miami and HSI Attaché Buenos Aires initiated an operation aimed at targeting transnational crime organizations involved in money laundering, trafficking of counterfeit merchandise, intellectual property rights violations, and contraband smuggling schemes from Paraguay, Brazil, and Argentina to the United States. Working in conjunction with its foreign counterparts, HSI TTU used legacy DARTTS to identify trade anomalies for numerous companies and suspect entities targeted by this operation. As of March 2013, these

enforcement actions have resulted in over 35 seizures of counterfeit registered trademarked goods with a manufacturer's suggested retail price of over 60 million USD. The operation has also resulted in nine seizures of weapons and weapons parts that were being illegally sent to Paraguay, including scopes, pistol parts, AR-15 rifle parts, shotguns, and, most notably, 50 medium machines guns.

A detailed discussion of the efficacy of FALCON-DARTTS will be included in future DHS Data Mining Reports.

6. Laws and Regulations

ICE is authorized to collect the information analyzed by FALCON-DARTTS pursuant to the Trade Act of 2002 § 343, 19 U.S.C. § 2071 Note; 19 U.S.C. § 1484; and 31 U.S.C. § 5316. ICE HSI has the jurisdiction and authority to investigate violations involving the importation or exportation of merchandise into or out of the United States. Information analyzed by FALCON-DARTTS supports, among other things, HSI's investigations into smuggling violations under 18 U.S.C. §§ 541, 542, 545, and 554; money laundering investigations under 18 U.S.C. § 1956; and merchandise imported in non-compliance with 19 U.S.C. §§ 1481 and 1484. DHS is authorized to maintain documentation of these activities pursuant to 19 U.S.C. § 2071 Note (Cargo Information) and 44 U.S.C. § 3101 (Records Management by Agency Heads; General Duties). Information analyzed by FALCON-DARTTS may be subject to regulation under the Privacy Act of 1974,[102] the Trade Secrets Act,[103] and the Bank Secrecy Act (BSA).

7. Privacy Impact and Privacy Protections

ICE does not use FALCON-DARTTS to make unevaluated automated decisions about individuals, and FALCON-DARTTS data is never used directly as evidence to prosecute crimes. FALCON-DARTTS is used solely as an analytical tool to identify anomalies. It is incumbent upon the HSI investigator to further investigate the reason for an anomaly. HSI investigators gather additional facts, verify the accuracy of the FALCON-DARTTS data, and use their judgment and experience to determine whether an anomaly is in fact suspicious and warrants further investigation for criminal violations. HSI investigators are required to obtain and verify the original source data from the agency that collected the information to prevent inaccurate information from propagating. All information obtained from FALCON-DARTTS is independently verified before it is acted upon or included in an HSI investigative or analytical report.

FALCON-DARTTS data is generally subject to access requests under the Privacy Act and FOIA, and requests for amendment under the Privacy Act, unless a statutory exemption covering specific data applies. U.S. and foreign government agencies that collect information analyzed by FALCON-DARTTS are responsible for providing appropriate notice on the forms used to collect the information, or through other forms of public notice, such as SORNs.[104] FALCON-

[102] 5 U.S.C. § 552a
[103] 18 U.S.C. § 1905.
[104] The following SORNs are published in the Federal Register and describe the raw data ICE receives from U.S. agencies for use in FALCON-DARTTS: for FinCEN Information, Suspicious Activity Report System (Treasury/FinCEN .002) and BSA Reports System (Treasury/FinCEN .003) (updates for both of these SORNs were

DARTTS will coordinate requests for access or to amend data with the original data owner. ICE published a PIA for FALCON-DARTTS on January 16, 2014. A republication of the SORN that applies to FALCON-DARTTS is forthcoming.[105]

All raw data analyzed by FALCON-DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority. Therefore, FALCON-DARTTS relies on the systems and/or programs performing the original collection to provide accurate data. The majority of the raw data used by FALCON-DARTTS is accurate, because the data was collected directly from the individual or entity to whom the data pertains. Due to the law enforcement context in which FALCON-DARTTS is used, however, there are often significant impediments to directly verifying the accuracy of information with the individual to whom the specific information pertains.[106] In the event that errors in raw data are discovered by FALCON-DARTTS users, the FALCON-DARTTS system owner will notify the originating agency. All raw data analyzed by FALCON-DARTTS is updated at least monthly for all sources, or as frequently as the source system can provide updates or corrected information.

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

The FALCON environment, of which FALCON-DARTTS is a component, was granted an ongoing Security Authorization on November 6, 2013. Any violations of system security or suspected criminal activity will be reported to the DHS Office of Inspector General, to the Office of the Information System Security Manager team in accordance with the DHS security standards, and to the ICE Office of Professional Responsibility.

As FALCON-DARTTS is a component system of the larger ICE HSI FALCON environment, FALCON-DARTTS uses the access controls, user auditing, and accountability functions described in the FALCON-SA PIA. For example, user access controls allow data access to be restricted at the record level, meaning that only datasets authorized for a user-specific profile are

published at77 FR 60014 (Oct. 1, 2012), available at http://www.gpo.gov/fdsys/pkg/FR-2012-10-01/pdf/2012-24017.pdf), and for CBP Information, ACE/International Trade Data System (DHS/CBP-001) (71 FR 3109 (Jan. 19, 2006), available at http://www.gpo.gov/fdsys/pkg/FR-2006-01-19/html/E6-511.htm), ACS (Treasury/CS.278) (73 FR 77759 (Dec. 19, 2008), available at http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29801.htm), and TECS (DHS/CBP-011) (73 FR 77778 (Dec. 19, 2008), available at http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm).

[105] FALCON-DARTTS is covered by the SORN for the ICE Trade Transparency and Analysis Research (TTAR) system of records (77 FR 53893 (Sept. 4, 2012)). Republication of the TTAR SORN to cover new datasets in FALCON-DARTTS, among other things, is scheduled for the third quarter of FY 2014. FALCON-DARTTS datasets not currently listed in the TTAR SORN are restricted from use in the system until the effective date of the updated SORN published in the *Federal Register*.

[106] For example, prior to an arrest, the agency may not have any communication with the subject because of the risk of alerting the subject to the agency's investigation, which could result in the subject fleeing or altering his or her behavior in ways that impede the investigation.

visible and accessible by that user. Audit capabilities log user activities in a user activity report, which is used to identity users who are using the system improperly.[107]

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

System access is granted only to ICE HSI, CBP, and foreign government personnel who require access to the functionality and data available in FALCON-DARTTS and its trade data subsystem in the performance of their official duties. Access is granted on a case-by-case basis by the FALCON-DARTTS Administrator, who is designated by the HSI TTU Unit Chief. User roles are reviewed regularly by a FALCON-DARTTS HSI supervisor to ensure that users have the appropriate access and that users who no longer require access are removed from the access list. All individuals who are granted user privileges are properly cleared to access information within FALCON-DARTTS and take system-specific training, as well as annual privacy and security training that stress the importance of authorized use of personal data in government systems.

In 2009, NARA approved a record retention period for the information maintained in the legacy DARTTS system. As noted in the 2014 FALCON-DARTTS PIA,[108] ICE intends to request NARA approval to retire the legacy DARTTS records retention schedule and incorporate the retention periods for data maintained in FALCON-DARTTS into the forthcoming records schedule for the FALCON environment. With this change, ICE will request to retain the FALCON-DARTTS datasets in the system for ten years. The proposed ten-year retention period for records is necessary to create a data set large enough to effectively identify anomalies and patterns of behavior in trade transactions. ICE will also request to retain the "inputs" to the FALCON-DARTTS system (i.e., the original raw data imported into FALCON-DARTTS from the source systems) for ten years to ensure data integrity and for system maintenance.

V. CONCLUSION

The DHS Privacy Office is pleased to provide the Congress its eighth comprehensive report on DHS data mining activities. The Congress has authorized the Department to engage in data mining in furtherance of the DHS mission while protecting privacy. The Office has reviewed the programs described in this report, using the compliance documentation process it requires for all DHS programs and systems to ensure that necessary privacy protections have been implemented. The DHS Privacy Office remains vigilant in its oversight of all Department programs and systems, including those that involve data mining.

[107] For more information on these controls, auditing, and accountability, see DHS/ICE/PIA-032A FALCON Search & Analysis System (FALCON-SA).

[108] Available at http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falcondartts_January 2014_0.pdf.

VI. APPENDIX

Acronym List	
ACAS	Air Cargo Advance Screening
ACE	Automated Commercial Environment
ACS	Automated Commercial System
ADIS	Arrival and Departure Information System
AES	Automated Export System
AFI	Analytical Framework for Intelligence
AFSP	Alien Flight Student Program
AMS	Automated Manifest System
APIS	Advance Passenger Information System
ATO	Authorization to Operate
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATS-AT	Automated Targeting System—Outbound Module
ATS-N	Automated Targeting System—Inbound Module
ATS-L	Automated Targeting System—Land Module
ATS-P	Automated Targeting System—Passenger Module
ATS-TF	Automated Targeting System—Targeting Framework
BCI	Border Crossing Information
BSA	Bank Secrecy Act
CBP	U.S. Customs and Border Protection
CCD	Consolidated Consular Database
CDC	Cross Domain Capabilities
CEI	Common Entity Index
CMAA	Customs Mutual Assistance Agreement
CMIR	The Report of International Transportation of Currency or Monetary Instruments Form
COTP	Captains of the Port
COTS	Commercial Off-The-Shelf
CRCL	Office of Civil Rights and Civil Liberties
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	U.S. Department of Homeland Security
DMV	Department of Motor Vehicles
DOJ	U.S. Department of Justice
DoS	U.S. Department of State
EBSVERA	Enhanced Border Security and Visa Entry Reform Act of 2002
EEI	Electronic Export Information
ENFORCE	ICE Enforcement Case Management System / Enforcement Integrated Database
ESTA	Electronic System for Travel Authorization

Acronym List	
FALCON-SA	FALCON Search & Analysis
FBI	Federal Bureau of Investigation
FinCEN	Department of the Treasury Financial Crimes Enforcement Network
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FY	Fiscal Year
HSI	ICE Homeland Security Investigations
HSI CPIU	ICE Homeland Security Investigations Counter-Proliferation Investigations Unit
I&A	DHS Office of Intelligence and Analysis
IAP	Immigration Advisory Program
ICE	U.S. Immigration and Customs Enforcement
IFS	Intelligence Fusion System
INA	Immigration and Nationality Act
IOC	Interagency Operations Center
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IT	Information Technology
LES	Law Enforcement Sensitive
MSB	Money Services Business
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NIIS	Nonimmigrant Information System
NTC	National Targeting Center
OFAC	Department of the Treasury Office of Foreign Asset Control
OGC	Office of General Counsel
OMB	Office of Management and Budget
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PNR	Passenger Name Record
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
RFI	Request for Information
SAFE Port Act	Security and Accountability for Every Port Act
SAVI	Suspect and Violator Indices
SBU	Sensitive But Unclassified
SELC	System Engineering Life Cycle
SEVIS	Student and Exchange Visitor Information System
SDN	Specially Designated Nationals
SORN	System of Records Notice
SSI	Sensitive Security Information

Acronym List	
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TSC	FBI Terrorist Screening Center
TSDB	Terrorist Screening Database
TS/SCI	Top Secret/Sensitive Compartmented Information
TTAR	Transaction and Analysis Research System
TTU	ICE Homeland Security Investigations Trade Transparency Unit
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
U.S.	United States
U.S.C.	United States Code
USCIS	United States Citizenship and Immigration Services
USCG	United States Coast Guard
USD	United States Dollar
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VSPTS-Net	Visa Security Program Tracking System
VWP	Visa Waiver Program