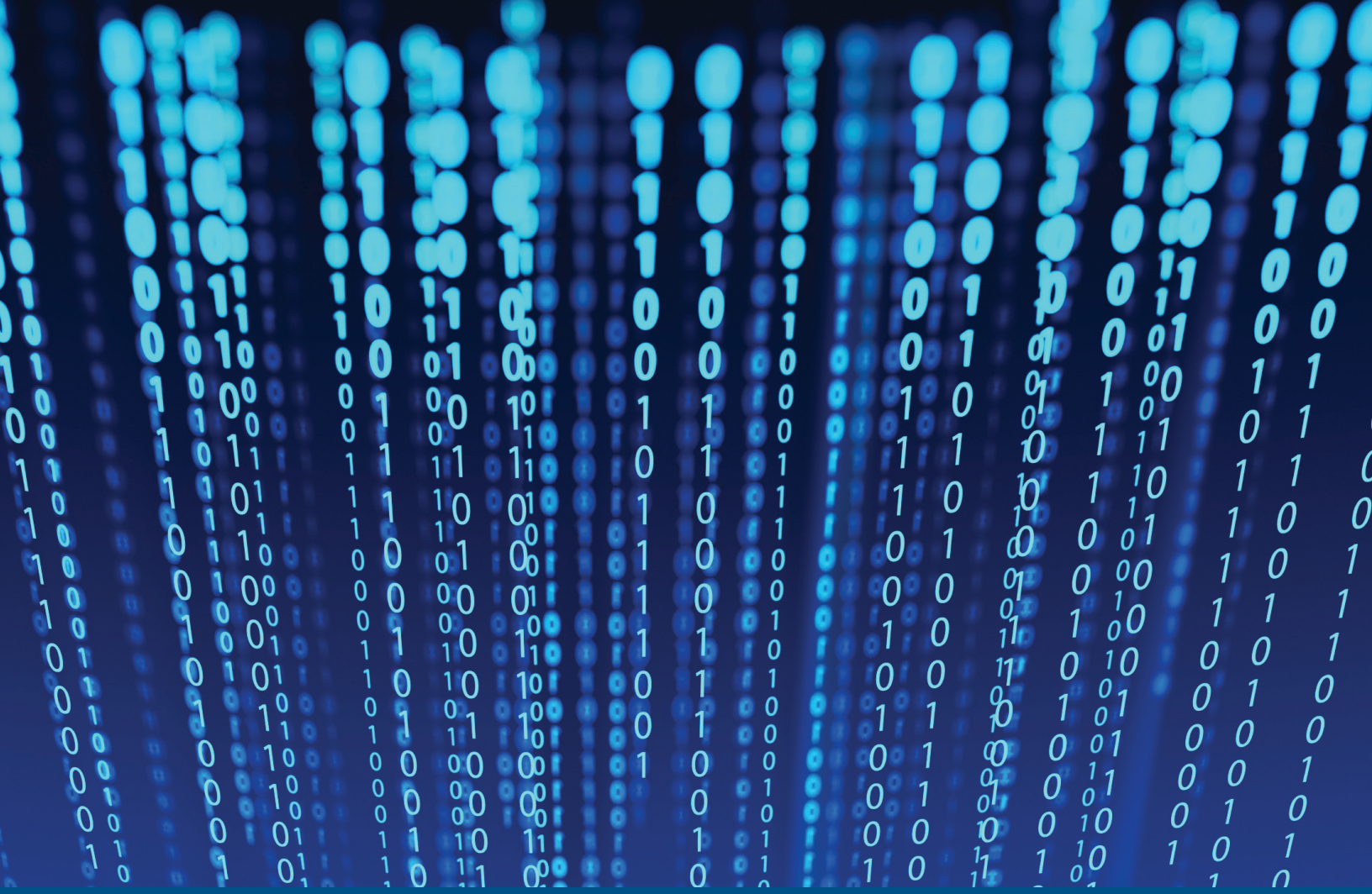

Department of Homeland Security

Privacy Office

2011 Data Mining Report to Congress

February 2012

Homeland Security

FOREWORD

February 2012

I am pleased to present the Department of Homeland Security's (DHS) 2011 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 1) a thorough description of the activity; 2) the technology and methodology used; 3) the sources of data used; 4) an analysis of the activity's efficacy; 5) the legal authorities supporting the activity; and 6) an analysis of the activity's impact on privacy and the protections in place to protect privacy. This is the sixth comprehensive DHS Data Mining Report, and the fourth report prepared pursuant to the Act. Two Annexes to this report that include Law Enforcement Sensitive information and Sensitive Security Information, respectively, are being provided separately to Congress as required by the Act.

When it created DHS, Congress authorized the Department to engage in data mining and other analytical tools in furtherance of Departmental goals and objectives. Consistent with the rigorous compliance process applied 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, United States Senate

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

The Honorable Joseph I. Lieberman
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins
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 Peter T. King
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 Lamar Smith
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,

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security

EXECUTIVE SUMMARY

The Department of Homeland Security Privacy Office (DHS Privacy Office or Office) is providing this report to Congress pursuant to the Department's obligations under section 804 of the Implementing the 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 2010 DHS Data Mining Report,[2] the DHS Privacy Office discussed three DHS programs that engage in activities that meet the Data Mining Reporting Act's definition of data mining: 1) the Automated Targeting System (ATS) Inbound (now called ATS-N), Outbound (now called ATS-AT), and Passenger (ATS-P) modules administered by U.S. Customs and Border Protection (CBP); 2) the Data Analysis and Research for Trade Transparency System (DARTTS) administered by U.S. Immigration and Customs Enforcement (ICE); and 3) the Freight Assessment System (FAS) administered by the Transportation Security Administration (TSA).

This year's report, covering the period December 2010 through November 2011, presents the complete descriptions of ATS-N, ATS-AT, and ATS-P, and DARTTS provided in the 2010 DHS Data Mining Report, with updates on modifications, additions, or other developments that have occurred in the current reporting year. This year's report also includes a new section on the Land module of ATS (ATS-Land), which now uses vehicle licensing information and ATS risk-based rules to assess the risk posed by vehicles and their occupants at U.S. land borders, and a brief summary of CBP's Analytical Framework for Intelligence (AFI), a strategic intelligence program currently in development.

The DHS Privacy Office has also identified three new uses of ATS by DHS Components in conjunction with CBP that are discussed below: the Air Cargo Advance Screening (ACAS) pilot (a joint effort of CBP and TSA); the DHS Overstay Initiative Pilot (involving ICE, the United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT), and CBP); and TSA's Secure Flight Program's use of ATS-P. Additional information on Secure Flight is being provided to Congress in a separate annex to this report that contains Sensitive Security Information.

As discussed in the 2010 Data Mining Report, FAS was developing a data mining capability to reduce reliance on random inspections for identifying cargo that could pose a heightened risk to passenger aircraft.[3] FAS did not deploy this capability, however, and no longer intends to do so. Therefore, FAS is not included in this year's report.

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.[4] DHS exercises its authority to engage in data mining in the programs discussed in this report, all of which have been reviewed by the DHS Chief Privacy Officer for potential impact on privacy.

[1] 42 U.S.C. § 2000ee-3.
[2] http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.
[3] 2010 Data Mining Report at 21, available at http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.
[4] 6 U.S.C. § 121(d)(14).

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);[5] the E-Government Act of 2002 (E-Government Act);[6] and section 222 of the Homeland Security Act, which states, in part, 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."[7]

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 and memorialized in *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*.[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) 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, before they become operational.[10] With the exception of AFI, all programs discussed in this report have issued PIAs and are covered by SORNs. AFI, which is not yet operational, is currently working with the Office to complete its PIA and SORN.

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 and that privacy protections have been implemented.

[5] 5 U.S.C. § 552a.
[6] Pub. L. No. 107-347.
[7] 6 U.S.C. § 142(a)(1).
[8] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[9] Pub. L. No. 107-347.
[10] 5 U.S.C. § 552a(e)(4).

DHS PRIVACY OFFICE
2011
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 Privacy Office (DHS Privacy Office or Office) is the first statutorily mandated privacy office in the Federal Government. Its mission is to preserve and enhance privacy protections for all individuals, promote transparency of DHS operations, and serve as a leader in the privacy community. 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 sixth comprehensive report to Congress on DHS activities that involve data mining, and the fourth 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,[16] the E-Government Act,[17] and the Homeland Security Act, which states, in part, 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 and memorialized in the December 2008 *Privacy Policy Guidance Memorandum 2008-01, The Fair*

[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 investigatory authority, the power to issue subpoenas, 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 2011 Annual Report to Congress* available at http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy_rpt_annual_2011.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 web site 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).

Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.[19] 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 main documents related to privacy compliance: (1) the Privacy Threshold Analysis (PTA); (2) the Privacy Impact Assessment (PIA);[20] and (3) the System of Record Notice (SORN).[21] While each of these documents has a distinct function in implementing privacy policy at DHS, together these documents further the transparency of Department activities and demonstrate accountability.

- **PTAs:** The PTA is the first document completed by a DHS Component seeking to implement or modify a system, program, technology, project, or rulemaking. The PTA identifies whether the system, program, technology, or project is privacy sensitive and thus requires additional privacy compliance documentation such as a PIA or SORN.
- **PIAs:** PIAs are an important tool for examining the privacy impact of IT systems, programs, technologies, projects, or rule-makings. The PIA is the method by which the DHS Privacy Office's Compliance Group reviews 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 a system of records, as well as insight into how information is used, retained, and may be corrected. Part of the Privacy Act analysis requires determining whether certain Privacy Act exemptions should be taken to protect the records from disclosure to an individual because of law enforcement or national security reasons. If a SORN is required, the program manager will work with the Component privacy officer or PPOC and Component counsel to write a SORN and submit 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.[22]

[19] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[20] The E-Government Act mandates PIAs for all federal agencies when there are new collections of, or new technologies applied to, PII. Pub. L. No. 107-347.
[21] 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).
[22] 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

The DHS Privacy Office identifies DHS programs that engage in data mining through several different processes. The Office reviews all Department OMB-300 budget submissions to learn of programs or systems that use PII and to determine whether they address privacy appropriately.[23] The Office uses the PTA to review all information technology systems that are going through the certification and accreditation (C&A) process required under the Federal Information Security Management Act of 2002 (FISMA)[24] to determine whether they maintain PII. The PIA process also provides the Office insight into technologies used or intended to be used by DHS. In addition, the Office reviews technology investment proposals that the DHS Enterprise Architecture Center of Excellence and Integrated Project Teams process, to ensure that DHS investments in technology include a specific review for compliance with privacy protection requirements. All of 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. With the exception of U.S. Customs and Border Protection's (CBP) Analytical Framework for Intelligence (AFI), which is not yet operational, all programs discussed in this report have issued PIAs and are covered by SORNs. CBP and the Office are working together to complete the AFI PIA and SORN, which will be issued before AFI begins operations.

review process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. The Privacy Act requires that SORNs be reviewed on a biennial basis.

[23] 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.

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

III. REPORTING

In the 2010 DHS Data Mining Report,[25] the DHS Privacy Office discussed three Department programs that engage in data mining as defined by the Data Mining Reporting Act: 1) the Automated Targeting System (ATS) Cargo Inbound (ATS-N), Cargo Outbound (ATS-AT), and Passenger (ATS-P) modules, which are administered by U.S. Customs and Border Protection (CBP); 2) the Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by U.S. Immigration and Customs Enforcement (ICE); and 3) the Freight Assessment System (FAS), which is administered by the Transportation Security Administration (TSA).

This year's report, covering the period December 2010 through November 2011, presents the complete descriptions of ATS-N, ATS-AT, and ATS-P, and DARTTS provided in the 2010 DHS Data Mining Report, with updates on modifications, additions, or other developments that have occurred in the current reporting year. This year's report also includes a new section on the Land module of ATS (ATS-Land), which now uses vehicle licensing information and ATS risk-based rules to assess the risk posed by vehicles and their occupants at U.S. land borders, and a brief summary of CBP's Analytical Framework for Intelligence (AFI), a strategic intelligence program currently in development.

The DHS Privacy Office has also identified three new uses of ATS by DHS Components in conjunction with CBP that are discussed below: the Air Cargo Advance Screening (ACAS) pilot (a joint effort of CBP and TSA); the DHS Overstay Initiative Pilot (involving ICE, the United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT), and CBP); and TSA's Secure Flight Program's use of ATS-P. Additional information on Secure Flight is being provided to the Congress in a separate annex that contains Sensitive Security Information.[26]

As discussed in the 2010 Data Mining Report, FAS was developing a data mining capability to reduce reliance on random inspections for identifying cargo that could pose a heightened risk to passenger aircraft.[27] FAS did not deploy this capability, however, and no longer intends to do so. Therefore, FAS is not included in this year's report.

A. Automated Targeting System (ATS)

1. 2011 Program Update

Several new developments took place with respect to ATS during the reporting period for this report:

[25] http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.
[26] The Data Mining Reporting Act requires federal agencies to report to Congress on the classified and law enforcement sensitive aspects of data mining activities in a separate non-public annex to their annual data mining reports. 42 U.S.C. § 2000ee-3(c)(3).
[27] 2010 Data Mining Report at 21, http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.

a) ATS Targeting Framework and ATS-Land

During this reporting period, CBP renamed a portion of the Intelligence and Operations Framework System (IOFS) module of ATS, which was discussed in the 2010 Data Mining Report,[28] as the Targeting Framework (ATS-TF), and is migrating the functionality supporting the strategic intelligence aspects of that module to a new system currently in development, the Analytical Framework for Intelligence (AFI), which is discussed below in section III.B. The creation of ATS-TF permits ATS to continue to maintain information pertaining to workflow, case management, and collaboration; the scope of this information, however, has been narrowed to address tactical or transactional incidents that require additional analysis or review. More comprehensive or strategic analysis and review of border incidents and intelligence will be moved under the scope of AFI. CBP is also expanding its use of the land border module for ATS (ATS-L). ATS-L supports screening of vehicles and passengers at the land border. Similar to the other modules in ATS, ATS-L employs targeting rules, in this case to identify vehicles and persons of interests based upon past border crossing activity and associations with known violators.

b) ATS-International

The 2010 Report noted that the ATS International module (ATS-I) was being developed to support collaborative efforts with foreign customs administrations.[29] ATS-I was designed to provide designated foreign customs authorities with controlled access to automated cargo targeting capabilities and a systematic medium for exchanging and developing best practices and targeting concepts. ATS-I is now an active sub-module affiliated with ATS-N. While ATS-I performs similar screening and targeting functions for foreign customs authorities using data and rule sets supplied by those authorities, the data in ATS-I is maintained separately from ATS-N and is not associated with U.S. data. The discussion below concerning the data mining aspects of ATS-N applies also to the manner in which ATS-I operates for CBP's foreign customs partners; however, ATS-I does not employ data inbound to the United States.

c) Secure Flight

TSA's Secure Flight Program (Secure Flight) began leveraging ATS-P to identify individuals requiring enhanced screening prior to boarding an aircraft. Secure Flight transmits instructions to the airlines identifying such individuals that are derived from real-time, threat-based intelligence rules run by ATS. More information about Secure Flight is included in the Secure Flight PIA, which was updated most recently on August 15, 2011.[30] 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)).

[28] 2010 Data Mining Report at 6, available at http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.
[29] 2010 Data Mining Report at 7, n. 7, available at http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.
[30] http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-secure-flight.pdf.

d) Overstay Vetting Pilot

DHS began a Department-wide Overstay Vetting Pilot using both the United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) overstay data maintained in the Arrival and Departure Information System (ADIS) and ATS-P 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 Pilot's goal is to allow ICE to deploy its investigative resources efficiently to locate high-risk overstays and initiate criminal investigations or removal proceedings against them. US-VISIT 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 US-VISIT, which, in turn, provides them to ICE for further processing. These activities are covered by existing PIAs for the ATS[31] and US-VISIT Technical Reconciliation Analysis Classification System.[32] US-VISIT also worked with the DHS Privacy Office to expand this existing coverage by completing a PIA specific to the Overstay Vetting Pilot to add another layer of analysis to this process that can be updated as the program matures. The PIA was published on December 29, 2011.

Legal authorities for the Overstay Vetting Pilot include: 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 (U.S.A. PATRIOT Act), Public Law 107–56; The Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Public Law 107–173; and The Immigration and Nationality Act (INA), 8 U.S.C. §§ 1185, 1225(as delegated by the Secretary of Homeland Security).

e) Air Cargo Advance Screening Pilot

CBP and TSA began a joint pilot, Air Cargo Advance Screening (ACAS), using existing CBP data collections and ATS-N to identify pre-departure air cargo that may pose a threat to aviation. 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, which amended 49 U.S.C. § 44901 to authorize TSA to screen cargo on passenger and all-cargo aircraft.

2. 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 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

[31] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf.
[32] See DHS/NPPD/USVISIT/PIA-004 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_tracs.pdf.

also uses ATS to identify other 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 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, as discussed below), ATS-P (which involves analysis of information about certain travelers, as discussed below), and the ATS Targeting Framework (ATS-TF) (a platform for temporary and permanent storage of data).[33]

During this reporting period, CBP renamed a portion of IOFS as ATS-TF. ATS-TF stores data that is being developed into an analytical product that may be permanently retained as a case within ATS-TF or shared with another system. ATS-TF permits review and cross referencing of analytical products and data from several different systems. ATS-TF permits CBP to relate information from several ATS modules (specifically ATS-P, ATS-L, and ATS-N) and portions of other CBP and federal agency systems (e.g., enforcement case tracking, Border Patrol Significant Incident Reports, and the Department of State's Consolidated Consular Database, and the Passport Information Electronic Records System) to support case development and collaboration between field and headquarters analytical staffs. ATS-TF supports the work of both Office of Field Operations officers and border patrol agents at ports of entry, in the field, and in the National Targeting Centers.

A legacy organization of CBP, the U.S. Customs Service, traditionally employed computerized screening 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 collected by carriers in connection

[33] The 2010 Data Mining Report noted two other ATS modules: ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP) (which provides trend analysis of historical international trade statistics to identify anomalous activity in aggregate) and ATS-International (ATS-I), which is being developed to support collaborative efforts with foreign customs administrations. ATS-TAP and ATS-I are no longer separate modules within ATS; they are now sub-modules under ATS-N. ATS-TAP does not employ data mining.

with a flight into or out of the United States, as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).[34]

ATS receives various data in real time from the following DHS and CBP mainframe systems: the Automated Commercial System (ACS), the Automated Manifest System (AMS), the DHS Advance Passenger Information System (APIS), the Automated Export System (AES), the Automated Commercial Environment (ACE), the DHS Electronic System for Travel Authorization (ESTA), the DHS Nonimmigrant Information System (NIIS), DHS Border Crossing Information (BCI), the DHS Student Exchange Visitor Information System (SEVIS) and TECS. TECS includes information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[35] Terrorist Screening Database (TSDB) and provides access to the Department of Justice National Crime Information Center (NCIC) regarding individuals with outstanding wants and warrants, and to Nlets, a clearinghouse for state wants and warrants as well as Departments of Motor Vehicle information. ATS collects PNR data directly from air carriers. ATS also collects data from certain express consignment services in ATS-N. ATS accesses data from these sources, which collectively include: electronically filed bills of lading, entries, and entry summaries for cargo imports; shippers' export declarations 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; nonimmigrant entry records; records from secondary referrals, incident logs, 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. Finally, ATS uses data from Dun & Bradstreet, a commercially available data source, to assist with company identification through name and address matching.

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 suspicious or unusual 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.

[34] 49 U.S.C. § 44909. The regulations implementing ATSA are codified at 19 C.F.R. § 122.49d.

[35] 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 in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, 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 use of terrorist information in screening processes. The TSC maintains the Federal Government's consolidated terrorist watch list, known as the TSDB.

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

i. Program Description

ATS-N assists CBP officers in identifying inbound cargo shipments that pose a high risk of containing weapons of mass effect, illegal narcotics, or other contraband, and in selecting that cargo for intensive examination. ATS-N is available to CBP officers at all major ports (i.e., air, land, sea, and rail) throughout the United States, and also assists CBP personnel in the Container Security Initiative (CSI) and Secure Freight Initiative (SFI) 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 Electronic Export Information (EEI) (formerly referred to as the Shippers' Export Declaration or SED) 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 and/or identifying exports that pose potential aviation safety and security risks (e.g., hazardous materials) or may be otherwise exported in violation of U.S. law.

ATS-N and ATS-AT look at data related to cargo in real time and engage in data mining to provide decision support analysis for 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 suspicious business activity generally. No decisions about individuals are made solely on the basis of these results.

The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) requires ATS to use or investigate the use of advanced algorithms in support of its mission.[36] To that end, ATS has established an Advanced Targeting Initiative, which includes plans for development of data mining, machine learning,[37] and other analytic techniques during the period from FY09 to FY12, for use in ATS-N and ATS-AT. Development will take place in iterative phases as the databases to be used by this initiative are updated. The various iterations will be deployed to a select user population, which will test the new functionality. The Advanced Targeting Initiative is being undertaken in tandem with ATS' maintenance and operation of the ATS-N and ATS-AT systems. As discussed in earlier DHS Data Mining Reports, the design and tool-selection processes for data mining, pattern recognition, and machine learning techniques in development

[36] 6 U.S.C. § 901.

[37] 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.

in the Advanced Targeting Initiative are under consideration and have yet to be finalized. Further details on this Initiative will be provided, as appropriate, in future Data Mining Reports.

iii. Data Sources

As noted above, ATS-N and ATS-AT do not collect information directly from individuals. The information maintained in ATS is either collected from private entities providing data in accordance with U.S. legal requirements (e.g., sea, rail, and air manifests) or is created by ATS as part of its risk assessments and associated rules.

ATS-N and ATS-AT use the information in ATS 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.[38] ATS-AT uses EEI data that exporters file electronically with AES, export manifest data from AES, export airway bills of lading, and census export data from the U.S. Department of Commerce 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 approach to detecting 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 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. By their very nature, the results produced by technologies used in the Advanced Targeting Initiative may be only speculative or inferential; they may only provide leads for further investigation rather than a definitive statement. It is valuable for the program to be able to very quickly produce useful leads gleaned from masses of information. Leads resulting in a positive, factual determination obtained through further investigation and physical inspections of cargo demonstrate the efficacy of these technologies.

[38] ATS-N collects information regarding individuals in connection with the following items including, but not limited to: Sea/Rail Manifests from AMS; Cargo Selectivity Entries and Entry Summaries from the Automated Broker Interface (ABI), a component of ACS; Air Manifests (bills of lading) from AMS; Express Consignment Services (bills of lading); CCRA Manifests (bills of lading from Canada Customs and Revenue (CCRA)); CBP Automated Forms Entry Systems (CAFES) 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 (FDA) Prior Notice (PN) requirements from ACS; and Census Import Data from the U.S. Department of Commerce.

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.[39] 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 counter-terrorism and drug law enforcement. ATS-AT also supports functions arising from the Anti-Terrorism Act of 1987[40] and the 1996 Clinger-Cohen Act.[41] The risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.[42]

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), to evaluate passengers and crew members prior to arrival or departure. ATS-P facilitates the CBP officer's decision-making process about whether a passenger or crew member should receive additional screening 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[43] and is subject to recurring systems maintenance. ATS-P is operational and has no set retirement date.

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

[39] *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.
[40] 22 U.S.C. § 5201 *et seq.*
[41] 40 U.S.C. § 1401 *et seq.*
[42] 6 U.S.C. § 912(b).
[43] 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 SLC has seven stages: initiation and authorization, project definition, system design, construction, acceptance and readiness, operations, and retirement.

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 a traveler's 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 does not make decisions about individuals solely based on the results of data mining in ATS-P. Rather, the CBP officer uses the information in ATS-P to assist in determining whether an individual should undergo additional inspection or should be allowed or denied admission into the United States.

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 screening relies upon information in APIS; NIIS (which contains all Form I-94 Notice of Arrival/Departure records); ESTA, which contains pre-arrival information for persons traveling from Visa Waiver Program (VWP)[44] countries (separately maintained in NIIS); the DHS Suspect and Violator Indices (SAVI); and the Department of State visa databases. ATS-P also relies upon PNR information from air carriers, BCI crossing data, seizure data, Report of International Transportation of Currency or Monetary Instrument Form (CMIR) data,[45] and information from the TSDB maintained by the TSC.

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 individual databases, and thereby helps facilitate 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 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 screening, or in some cases, denied them boarding. ATS-P matches have also enabled CBP officers and foreign law enforcement partners to disrupt and apprehend persons engaged in

[44] 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 section 217 of the Immigration and Nationality Act, 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.

[45] The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.

human trafficking and drug smuggling operations. For example, in one coordinated effort during Fiscal Year 2011, there were 639 identifications and adverse actions taken against persons identified as being involved in human trafficking. ATS-P also remains an effective tool in preventing child abductions involving individuals who are attempting to flee the United States in violation of a court order.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.[46] 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, where appropriate, admissibility to the satisfaction of the CBP officer and then submit to inspection for customs purposes. The information collected is authorized pursuant to the Enhanced Border Security and Visa Reform Act of 2002,[47] ATSA, the Intelligence Reform and Terrorism Prevention Act of 2004,[48] the Immigration and Nationality Act, as amended,[49] and the Tariff Act of 1930, as amended.[50] 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 supports CBP Officers and Border Patrol Agents at the land border with access to real-time screening and targeting databases to assess the risk posed by vehicles and their occupants as they cross the border. The module employs data obtained from CBP license plate readers and traveller documents to compare information against state department of motor vehicles (DMV) databases and ATS screening datasets to assess risk and to determine if a vehicle or person travelling in it should be investigated further. 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 travellers through the border crossing process.

ii. Technology and Methodology

ATS-L processes vehicle and occupant information against other information 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 weighting positive and negative results from subject matter expert rules), or affiliate rules (derived from data establishing an association with a known violator). The subject matter expert rules 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 past crossing

[46] *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.
[47] Pub. L. No. 107-173.
[48] Pub. L. No. 108-458.
[49] 8 U.S.C §§ 1185,1225.
[50] 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.

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 a person's 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 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 or be allowed admission into the United States.

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 screening relies upon information in NIIS, ESTA, SAVI, and the Department of State 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 maintained by the TSC.

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 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, and thereby helps facilitate the more efficient movement of vehicles and occupants 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 and occupants. 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.[51] 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, where appropriate, admissibility to the satisfaction of the CBP officer and must submit to inspection for customs purposes. Information collection in ATS-L is pursuant to the authorities for information collection in ATS-P, i.e., the Enhanced Border Security and Visa Reform Act of 2002,[52] ATSA, the Intelligence Reform and Terrorism Prevention Act of 2004,[53]

[51] *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.
[52] Pub. L. No. 107-173.
[53] Pub. L. No. 108-458.

Immigration and Nationality Act, as amended,[54] and the Tariff Act of 1930, as amended.[55] 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.

3. ATS Privacy Impacts and Privacy Protections

The Privacy Office has worked closely with CBP to ensure that ATS satisfies the privacy compliance requirements for operation. CBP completed a PIA and published a SORN for ATS in August 2007 and is currently updating both documents.[56] 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.[57] 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 immediately 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.[58]

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, a redress process has been developed. 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 from the United States that provides CBP's Pledge to Travelers. This pledge gives each traveler

[54] 8 U.S.C §§ 1185,1225.
[55] 19 U.S.C. §§ 66, 1433, 1454, 1485, 1624, and 2071.
[56] The PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf. The SORN is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_sorn_cbp_ats_fromFR.pdf, and in the Federal Register at 72 Fed. Reg. 43650 (Aug. 6, 2007). CBP published an update to the PIA in December 2008 to reflect new requirements regarding information pertaining to cargo to be submitted by importers and vessel carriers before the cargo is brought to the U.S. by vessel. The PIA update is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate10plus2.pdf. CBP published a final rule for Privacy Act exemptions for ATS in the Federal Register on February 3, 2010 (75 Fed. Reg. 5487). The final rule is also available at http://www.dhs.gov/files/publications/gc_1185458955781.shtm#3.
[57] 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 in support of their authorized intelligence activities in accordance with applicable law, Executive Orders, and policy.
[58] 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.

an opportunity to speak with a passenger service representative to answer any questions about CBP procedures, requirements, policies, or complaints.[59] 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, with respect to 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, government-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, a traveler can seek correction of erroneous PNR information stored in ATS and information stored in other DHS databases.[60]

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. Individuals may gain access to their own data from 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.[61] Privacy Act and FOIA requests for access to information for which ATS is the source system are directed to CBP.[62]

ATS underwent the C&A process in accordance with DHS and CBP policy and obtained its initial C&A 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 C&A and Security Risk Assessment were subsequently updated and are valid until January 21, 2014.

Access to ATS is audited periodically 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.

[59] In addition, travelers can visit CBP's Customer Service web site 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 Customer Service Center and the telephone number of the Joint Intake Center. Travelers may also file complaints through the DHS Traveler Redress Inquiry Program (DHS TRIP) by visiting the DHS TRIP website at http://www.dhs.gov/xtrvlsec/programs/gc_1169676919316.shtm.

[60] DHS TRIP can be accessed at: http://www.dhs.gov/files/programs/gc_1169676919316.shtm (*see*, 72 Fed. Reg. 2294, January 18, 2007).

[61] 5 U.S.C. § 552.

[62] 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, or by phone to the CBP FOIA office is (202) 325-0150.

As discussed above, ATS both 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' National Archives and Records Administration (NARA)-approved record retention schedule, except as noted below.[63] The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for an additional eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. These time periods may be modified in the future, depending on the new SORN standards and international agreements.

Notwithstanding the foregoing, information maintained only in ATS that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (i.e., specific and credible threats, and 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)

CBP is currently developing the Analytical Framework for Intelligence (AFI), a system that, as understood at the close of the reporting period for this report, will include a data mining capability as defined by the Data Mining Reporting Act. AFI will house the strategic intelligence functions formerly used by IOFS (now ATS-TF) and, when fully developed, will support CBP intelligence efforts to detect, locate, analyze, and counteract terrorist networks, drug trafficking networks, and other similar threats to the United States. Current plans for AFI include an analytical capability that will allow analysts 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. The development of this analytical capability is ongoing. Further details will be provided in the PIA and SORN for AFI that were nearing completion as the reporting period for this report ended, and, as appropriate, in future Data Mining Reports.

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

1. 2011 Program Update

During the current reporting period, ICE's Office of Homeland Security Investigations (HSI)[64] added two data sources to DARTTS. The first is the Specially Designated Nationals List (SDN List) created and maintained by the Office of Foreign Asset Control (OFAC) at the U.S. Department of the Treasury. The SDN List is a public record maintained on the Treasury website. The second is subject records from the TECS system that were created by HSI users in

[63] NARA approved the record retention schedule for ATS on April 12, 2008.
[64] HSI, formerly known as the Office of Investigations, was established during ICE's internal re-organization in June 2010.

furtherance of investigations. The subject records contain information about particular subjects of HSI-led investigations, such as persons, businesses, and vehicles.

ICE also initiated steps to expand the use of DARTTS in the coming year to include select CBP customs officers and import specialists. Once implemented, these CBP users will have privileges to access and analyze all trade data in DARTTS but will not have privileges to access the financial data in DARTTS. CBP will use DARTTS to support its mission to enforce U.S. trade laws and ensure the collection of all lawfully owed revenue from trade activities. Specifically, CBP will use DARTTS to identify anomalous transactions that may indicate violations of U.S. trade laws. If ICE elects not to open an investigation into these transactions, CBP may initiate administrative actions to recover delinquent revenue or penalties. Before initiating formal administrative action, CBP will first follow up on the anomalous transactions to determine if they are in fact suspicious and warrant further inquiry. CBP personnel will gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination. Not all anomalies identified in DARTTS will lead to CBP administrative actions.

In the coming year, ICE will also change the means by which foreign partners access anonymized U.S. trade data. Currently, ICE purchases a license for DARTTS software for select foreign partners that have established Trade Transparency Units (TTUs) in their own governments. These foreign partners use stand-alone computers to host DARTTS, which is loaded with anonymized U.S. trade data as well as the foreign partner's own trade data. ICE has supported the operation of these foreign instances of DARTTS by traveling to the foreign partner's office to update software and load new data into the system. To reduce costs and improve the security of these foreign instances of DARTTS, in the next year ICE will begin migrating each stand-alone foreign instance of DARTTS to an Internet-based version of DARTTS hosted on the ICE network. Once deployed, each foreign partner will access only its own foreign instance of DARTTS online using ICE-supplied user credentials; there will be no change in the data accessed or in the analytical tools. Using a secure FTP server, each foreign partner will continue to supply ICE with its own country's trade data, which ICE will upload into the U.S. DARTTS system as well as the foreign instance of DARTTS. The foreign instance of DARTTS will be maintained separately from the U.S. instance of the system. DARTTS will also provide data isolation features (roles) assigned to each foreign user to ensure that there is no comingling of country data among these users. Additional information about ICE's future plans for DARTTS is included in an annex to this report that contains Law Enforcement Sensitive information and is being provided separately to the Congress.

ICE is in the process of drafting a PIA Update for DARTTS to address these new data sources, and to describe the planned future use of DARTTS by CBP and foreign partners. ICE published its current PIA on April 26, 2010.[65]

2. Program Description

ICE maintains DARTTS, which generates leads for and otherwise supports HSI investigations of trade-based money laundering, contraband smuggling, trade fraud, and other import-export crimes. DARTTS analyzes trade and financial data to identify statistically anomalous

[65] The DARTTS PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_dartts2.pdf.

transactions that may warrant investigation. These anomalies are then independently confirmed and further investigated by experienced HSI investigators.

DARTTS is owned and operated by the ICE HSI Trade Transparency Unit (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 contraband smuggling, trafficking of counterfeit goods, misclassification of goods, and the over- or under-valuation of goods to hide the proceeds of illegal activities. 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. DARTTS is designed specifically to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator.

DARTTS allows HSI to perform research and analysis that is not available in any other ICE system because of the data it contains and the level of detail at which the data can be analyzed.[66] 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 that has been pre-determined to be suspect). Instead, it identifies trade and financial transactions that are statistically anomalous based on user-specified queries. Investigators follow up on the anomalous transactions to determine if they are in fact suspicious and warrant further investigation. Investigators gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination. Not all anomalies lead to formal investigations.

DARTTS is currently used by HSI Special Agents and Criminal Research Specialists who work on TTU investigations at ICE Headquarters or in the ICE HSI field and foreign attaché offices, as well as properly cleared support personnel. DARTTS is accessible to HSI users via the ICE enterprise network.

3. Technology and Methodology

DARTTS uses trade data collected by CBP, other federal agencies and foreign governments, and financial data collected by CBP and FinCEN. DARTTS data are primarily related to international commercial trade and financial transactions. ICE does not collect information directly from individuals or entities for inclusion in DARTTS. Instead, ICE receives data from the sources listed below via CD-ROM, external storage devices, or electronic data transfer and loads the data into DARTTS. DARTTS uses COTS software to analyze raw trade and financial data to identify anomalies and other suspicious transactions. The software application is designed for experienced investigators. It enables the analysis of structured and unstructured data using three tools: the drill-down technique,[67] link analysis, and charting and graphing tools

[66] For instance, DARTTS allows investigators to view totals for merchandise imports and then sort on any number of variables, such as country of origin, importer name, manufacturer name, or total value.

[67] The drill-down system allows 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. Investigators can also connect from one dataset within DARTTS to another, to see whether the suspicious people, entities, or patterns occur elsewhere.

that use proprietary statistical algorithms.[68] It also allows non-technical users with investigative experience to analyze large quantities of data and rapidly identify problem areas. The program makes it easier for investigators to apply their specific knowledge and expertise to complex sets of data.

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 goods, which may be an indicator of trade-based money laundering. 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.

DARTTS routinely receives bulk financial and trade information collected by other agencies and foreign governments,[69] hereafter referred to as "raw data." The sources of the raw data are described below. The agencies that provide DARTTS with trade data collect any PII directly from individuals or enterprises completing import-export electronic or paper forms.[70] Agencies that provide DARTTS with financial data receive PII from individuals and institutions, such as banks, that are required to complete certain financial reporting forms.[71] 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 analyses to identify possible criminal activity and provide support to field investigators. TTU investigators at ICE Headquarters refer the results of DARTTS analyses to ICE 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 DARTTS analyses. HSI investigators in attaché offices at U.S. embassies abroad have access to DARTTS on stand-alone terminals. These investigators use DARTTS to conduct analyses in support of financial, money laundering, and trade fraud investigations, and to respond to inquiries from partner-country TTUs with whom ICE shares anonymized U.S. trade data.

[68] DARTTS provides investigators the means to represent data graphically in graphs, charts, or tables to make identification of anomalous transactions easier and visually obvious. DARTTS does not create new records to be stored in DARTTS.

[69] 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.

[70] 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.

[71] U.S. 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.

4. Data Sources

All raw data in 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, U.S. financial data, and law enforcement records. U.S. trade data in DARTTS 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) export data that CBP and the U.S. Department of Commerce collect from individuals and entities exporting commodities from the United States using Commerce Department Form 7525-V (Shipper's Export Declaration) or through AES;[72] and 3) publicly available aggregated U.S. export data (i.e., data that does not include PII) purchased by ICE from the U.S. Department of Commerce.[73] In the DARTTS enterprise version, ICE began testing a new data module with bill of lading data, i.e., data provided by carriers to confirm the receipt and transportation of on-boarded cargo to a specified destination. This information includes consignee name and address, shipper name and address, container number, carrier, and bill of lading. It is collected by CBP via AMS, and is provided to ICE through CD-ROM, external storage devices, or electronic data transfers for uploading into DARTTS. ICE updated the DARTTS PIA to include the new bill of lading module on April 26, 2010.[74]

Foreign import and export data in DARTTS is provided to ICE by partner countries pursuant to a Customs Mutual Assistance Agreement (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 for uploading into DARTTS. This data is in the form of the following financial transaction reports: CMIRs; Currency Transaction Reports (deposits or withdrawals of more than $10,000 in currency into or from depository institutions and casinos and card clubs); Suspicious Activity Reports (information regarding suspicious financial transactions within depository institutions, money services businesses,[75] the securities and futures industry, and casinos and card clubs); Reports of Cash Payments over $10,000 Received in a Trade or Business (reports of merchandise purchased with $10,000 or more in currency); and data provided in Reports of Foreign Bank and Financial Accounts (FBAR) (reports by U.S. persons who have financial interest in, or signature or other authority over, foreign financial accounts in excess of $10,000).

ICE receives law enforcement records from two sources. First, ICE ingests into DARTTS the publicly available SDN List, which is a list of individuals and companies owned or controlled

[72] AES is operated jointly by the U.S. Census Bureau and CBP.
[73] This dataset is known as the U.S. Exports of Merchandise Dataset and is further described (including a complete list of data fields) on the U.S. Department of Commerce website available at http://www.census.gov/foreign-trade/reference/products/catalog/expDVD.html.
[74] The PIA is available on the Privacy Office website at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_dartts2.pdf.
[75] Money services businesses are required by the BSA to complete and submit Suspicious Activity Reports to FinCEN. 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 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.

by, or acting on behalf of, targeted countries. The list also contains information about foreign individuals, groups and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Such individuals and companies are called "Specially Designated Nationals." Their assets are blocked and U.S. persons and entities are generally prohibited from dealing with them. This dataset is compiled and maintained by OFAC and is also publicly available on the OFAC website.[76] The inclusion of the SDN List into DARTTS allows HSI users to rapidly determine, while using DARTTS to conduct analysis, if international trade and/or financial transactions with a specially designated individual or entity are being conducted, thus providing HSI with the ability to take appropriate actions in a timely and more efficient manner.

Second, ICE ingests into DARTTS subject records created by HSI users from CBP's TECS database. HSI subject records pertain to subjects (persons), vehicles, vessels, businesses, aircraft, and 'things' (houses, etc.). Having HSI subject records in DARTTS allows HSI investigators to quickly determine if an entity that is being researched in DARTTS is already part of a pending investigation or was involved in an investigation that is now closed. Currently, HSI investigators check TECS manually for this information. Inclusion of these records in DARTTS will improve the efficiency of HSI investigations.

DARTTS itself is the source of analyses of the raw data produced using COTS software analytical tools within the system. DARTTS also creates extracts of U.S. trade data that has been stripped of PII, and provides those extracts to partner countries that operate their own TTUs and have DARTTS terminals set up within their customs agencies' offices. This trade data is shared only with partner countries that have entered into a CMAA or other similar agreement with the United States. U.S. financial data in DARTTS is not shared with partner countries.

5. Efficacy

DARTTS has proved to be a useful tool for HSI in identifying criminal activity. To date, the HSI TTU has initiated several case referrals and continues to support ongoing investigations. Information from DARTTS has assisted in several criminal prosecutions. For example, using information gathered through DARTTS, HSI was able to disrupt a criminal organization involved in the illegal exportation of electronics to a U.S.-designated terrorist entity in Paraguay. Three defendants were arrested in February 2010 for charges including violation of the International Emergency Economic Powers Act (IEEPA), smuggling electronic goods from the United States to Paraguay, and conspiracy. On October 20, 2010, all three defendants pled guilty to the export smuggling and conspiracy charges.

Between 2008 and 2010, information from DARTTS was used to assist in an investigation into a California-based company that sold stuffed animals but was also involved in a money laundering organization responsible for narcotics trafficking between the United States and Colombia. HSI was able to disrupt, dismantle, and ultimately stop the money laundering organization by using data obtained from DARTTS and research and analysis provided by the TTU. In 2010, the investigation culminated in the indictment and arrest of three officers in the company for conspiracy to defraud the United States and the seizure of evidence related to money laundering.

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

6. Laws and Regulations

ICE is authorized to conduct these law enforcement activities under 18 U.S.C. § 545 (Smuggling goods into the United States); 18 U.S.C. § 554 (Smuggling goods from the United States); 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); 19 U.S.C. § 1484 (Entry of Merchandise); and 50 U.S.C. §§ 1701-1706 (the International Emergency Economic Powers Act.) 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 in DARTTS is regulated under the Privacy Act of 1974, the Trade Secrets Act,[77] and the Bank Secrecy Act (BSA).

7. Privacy Impact and Privacy Protections

ICE does not use DARTTS to make unevaluated automated decisions about individuals, and DARTTS data is never used directly as evidence to prosecute crimes. DARTTS is solely an analytical tool that helps in the identification of anomalies. It is incumbent upon the investigator who finds an anomaly to further investigate the reason for the anomaly. If the anomaly can be legitimately explained, the investigator has no need to further investigate it for criminal violations and moves on to the next identifiable anomaly. 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 DARTTS is independently verified before it is acted upon or included in an HSI investigative or analytical report. Investigators follow up on anomalous transactions to determine if they are in fact suspicious and warrant further investigation. They gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination.

DARTTS data is generally subject to access and amendment requests under the Privacy Act of 1974 and FOIA, unless a statutory exemption covering specific data applies. U.S. and foreign government agencies that collect information uploaded into 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.[78] DARTTS will coordinate requests for access or to mend data with the original data owner. During the coming year, ICE plans to work closely with the Privacy Office to complete and publish an updated PIA and SORN for DARTTS.[79]

As all of the information in DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority, DARTTS cannot independently verify the accuracy of the data it receives. The owner of the source data is responsible for maintaining and checking the accuracy of its own data. In many instances, the data ultimately loaded into DARTTS is highly accurate because it is collected directly from the individual. In other instances, however, the data about individuals is provided to a governmental organization by a third party. In the event that errors are found, the DARTTS system owner must notify the

[77] 18 U.S.C. § 1905.

[78] The following SORNs are published in the Federal Register and describe the raw data ICE receives from U.S. agencies for use in DARTTS: for FinCEN Information, Suspicious Activity Report System (Treasury/FinCEN .002) and BSA Reports System (Treasury/FinCEN .003); for Commerce Department Information, Individuals Identified in Export Transactions System (Commerce/ITA-1); and for CBP Information, Automated Commercial Environment/International Trade Data System (ACE/ITDS) (DHS/CBP-001).

[79] DARTTS is covered by the SORN for the ICE Trade Transparency and Analysis Research (TTAR) system of records. The SORN is available on the Privacy Office website at http://www.dhs.gov/privacy and in the Federal Register at 74 FR 39083 (August 5, 2009).

agency that originally collected the data. FinCEN currently provides ICE with corrections to existing data, which are then uploaded into DARTTS. ICE does not, however, receive data corrections on trade data.

DARTTS re-certified its C&A and was granted a three-year authority to operate from DHS IT Security on April 22, 2010. In 2010, DARTTS completed its transition to the ICE enterprise network and is now maintained within the secure DHS network firewall. 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.

All DARTTS users are assigned unique user IDs and passwords. Audit trails are used to track the date and time of login and sequences of users' actions and queries. New audit trail functionality has been implemented to provide an even more detailed trail and a higher level of integrity and accountability. The new audit trail features for the DARTTS enterprise version automatically track each action that occurs in the system, the date and time the action occurs, and which user performed the action. Only authorized personnel have access to audit trails, which are kept for a minimum of 90 days. Audit trails are reviewed by DARTTS system administrators and the Information System Security Officer. The system administrator also maintains a spreadsheet record of the receipt or distribution of sensitive information on electronic media.[80]

Access to DARTTS is granted on a case-by-case basis by the TTU Network Administrator. Access is currently limited to HSI users working on TTU investigations, as well as properly cleared support personnel. Future planned users are select CBP customs officers and import specialists. Once a foreign instance of DARTTS is deployed, foreign government customs officers and import specialists will also be granted access where ICE has diplomatic agreements or arrangements with that government's Trade Transparency Unit. The specific procedures for how those users will be approved for DARTTS access are still being determined. All individuals who are granted system use privileges are properly cleared to access information within DARTTS.

In 2009, NARA approved a record retention period for the information maintained in DARTTS. ICE maintains records in DARTTS for five years and then archives them for five additional years, for a total retention period of 10 years. In the coming year, ICE will propose to modify that retention period to retain the data for a total of ten years in the system. A retention policy change from five to ten years' worth of data in the system would provide more useful analytical results to DARTTS users and would permit them to view transactions of ongoing trade-based or financial fraud over a more significant period of time. 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. Original CD-ROMs containing raw data will be retained for five years to ensure data integrity and for system maintenance.

[80] DARTTS receives CD-ROMs and other external storage media provided by other agencies. Once data from CD-ROMs or other external storage media is loaded onto DARTTS, the TTU Network Administrator stores them in the secured server room located in the TTU offices at ICE Headquarters until the retention period has elapsed, at which point they are destroyed.

D. Freight Assessment System (FAS)

1. 2011 Program Update

As discussed in the Department's earlier Data Mining Reports, the TSA Freight Assessment System (FAS) is a risk-assessment tool that was intended to be used to identify cargo that may pose a heightened risk to passenger aircraft. FAS was originally designed to reduce reliance on random inspections conducted by industry by using machine-derived rules and predictive indicators to identify and assess high-risk cargo. As part of its implementation of the 100-percent screening requirements of the Implementing Recommendations of the 9/11 Act, TSA has not and does not expect to deploy data-mining capabilities to identify air cargo for further inspection. A complete description of FAS as originally designed is included in the Department's 2008, 2009, and 2010 Data Mining Reports.

IV. CONCLUSION

The DHS Privacy Office is pleased to provide the Congress its sixth 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 DHS programs and systems generally 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.

V. APPENDICES

A. Acronym List

Acronym List	
ACE	Automated Commercial Environment
ACS	Automated Commercial System
AES	Automated Export System
AMS	Automated Manifest System
APIS	Advance Passenger Information System
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATS-P	ATS Passenger Module
BCI	Border Crossing Information
BSA	Bank Secrecy Act
C&A	Certification and Accreditation
CBP	United States Customs and Border Protection
CMAA	Customs Mutual Assistance Agreement
CMIR	The Report of International Transportation of Currency or Monetary Instruments Form
COTS	Commercial Off-The-Shelf
CSI	Container Security Initiative
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	Department of Homeland Security
EEI	Electronic Export Information
ESTA	Electronic System for Travel Authorization
FAS	Freight Assessment System
FBAR	Report of Foreign Bank and Financial Accounts
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
HSI	ICE Homeland Security Investigations Directorate
I&A	Office of Intelligence and Analysis
ICE	Immigration and Customs Enforcement
IEEPA	International Emergency Economic Powers Act
IOFS	Intelligence and Operations Framework System
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NIIS	Nonimmigrant Information System
OFAC	Office of Foreign Asset Control, U.S. Department of the Treasury
PIA	Privacy Impact Assessment

Acronym List	
PII	Personally Identifiable Information
PNR	Passenger Name Record
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
SAVI	Suspect and Violator Indices
SED	Shippers' Export Declaration
SELC	System Engineering Life Cycle
SFI	Secure Freight Initiative
SORN	System of Records Notice
TSA	Transportation Security Administration
TSC	FBI Terrorist Screening Center
TSDB	Terrorist Screening Database
TTU	ICE Office of Investigations Trade Transparency Unit
USCIS	United States Citizenship and Immigration Services
VWP	Visa Waiver Program