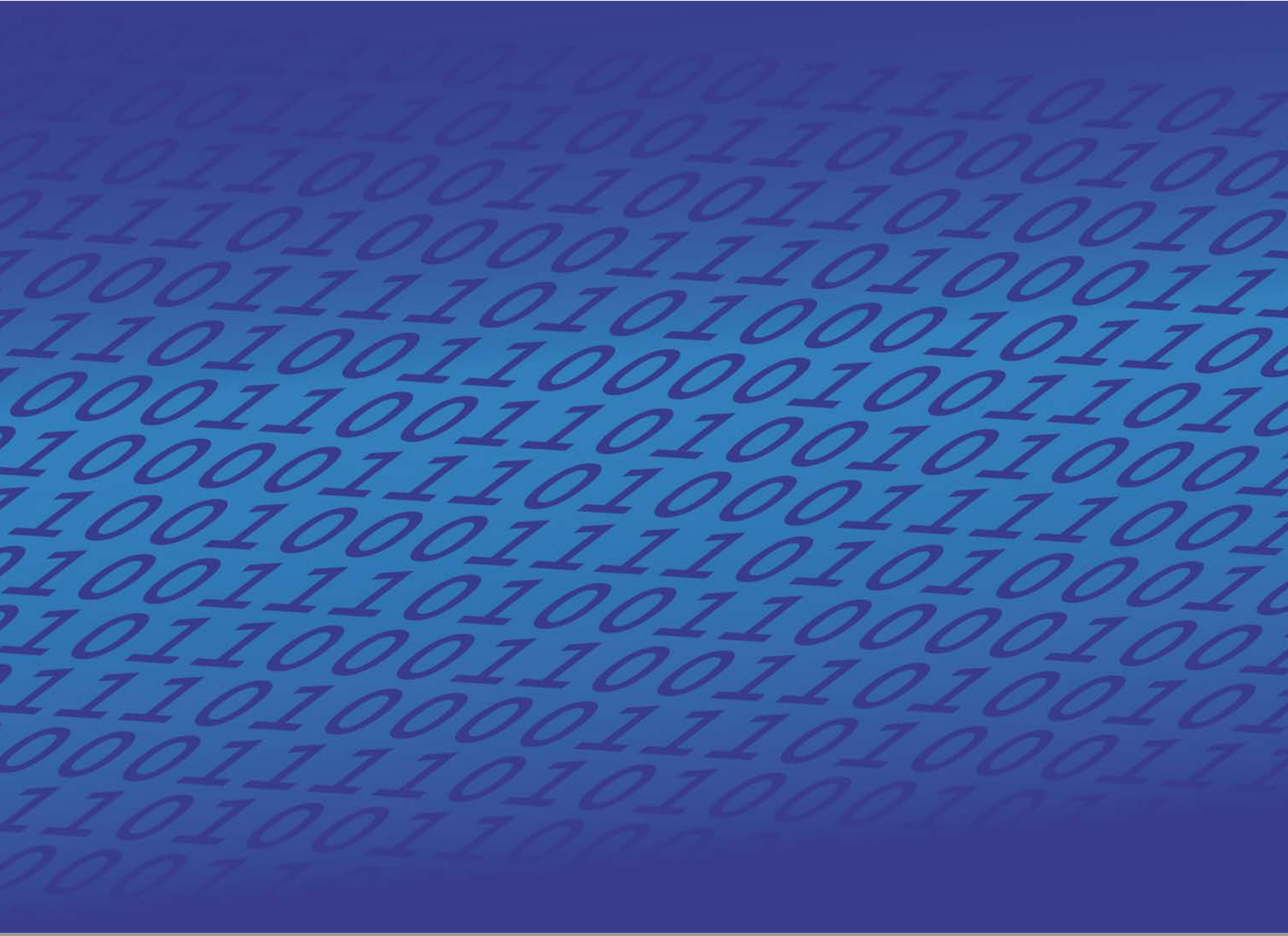

Department of Homeland Security

Privacy Office

2014 Data Mining Report to Congress

January 2015

FOREWORD

January 2015

I am pleased to present the Department of Homeland Security's (DHS) 2014 Data Mining Report to Congress. The Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3, requires DHS to report annually to Congress on DHS activities that meet the Act's definition of data mining.

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

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

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

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

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

The Honorable Ron Johnson
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

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

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

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

The Honorable Richard Burr
Chairman, U.S. Senate Select Committee on Intelligence

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

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

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

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

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

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

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

The Honorable Devin Nunes
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Adam Schiff
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

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

Sincerely,

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

EXECUTIVE SUMMARY

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

In the 2013 DHS Data Mining Report,[2] the DHS Privacy Office discussed the following Department programs that engage in data mining, as defined by the Data Mining Reporting Act:

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

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

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

(4) The FALCON-Roadrunner system, which is administered by ICE; and

(5) The DHS Data Framework, which is a DHS-wide initiative.

This year's report, covering the period January 1, 2014, through December 31, 2014, provides updates on modifications, additions, and other developments that have occurred in the current reporting year including use of ATS by DHS components other than CBP. The report also provides updates on two programs first discussed last year that include data mining capabilities: FALCON-Roadrunner, which is administered by ICE, and the DHS Data Framework, which is a DHS-wide initiative. Additional information on DARTTS and on the Transportation Security Administration's (TSA) Secure Flight Program's use of ATS is being provided separately to Congress in two annexes to this report that contain Law Enforcement Sensitive Information and Sensitive Security Information, respectively.

The Homeland Security Act of 2002, as amended (Homeland Security Act), expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[3] DHS exercises its authority to engage in data mining in the programs discussed in this report, all of which the DHS Chief Privacy Officer has reviewed for their potential impact on privacy. The Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974, as amended (Privacy Act);[4] the E-Government Act of 2002 (E-Government Act);[5] and Section 222 of the Homeland Security Act, which states that the Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies

[1] 42 U.S.C. § 2000ee-3.
[2] http://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf.
[3] 6 U.S.C. § 121(d)(13).
[4] 5 U.S.C. § 552a.
[5] Pub. L. No. 107-347.

sustain[s], and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."[6]

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

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

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

[6] 6 U.S.C. § 142(a)(1).

[7] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[8] Directive 047-01 and its accompanying Instruction are available at https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf and https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-instruction-047-01-001.pdf, respectively. The Directive supersedes DHS Directive 0470.2, *Privacy Act Compliance*, which was issued in October 2005.

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

[10] 5 U.S.C. § 552a(e)(4).

DHS PRIVACY OFFICE

2014 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 of the Act's reporting requirement. Two aspects of the Act's definition of "data mining" are worth emphasizing. First, the definition is limited to pattern-based electronic searches, queries, or analyses. Activities that use only PII or other terms specific to individuals (e.g., a license plate number) as search terms are excluded from the definition. Second, the definition is limited to searches, queries, or analyses that are conducted for the purpose of identifying predictive patterns or anomalies that are indicative of terrorist or criminal activity by an individual or individuals. Research in electronic databases that produces only a summary of historical trends, therefore, is not "data mining" under the Act.

II. Data Mining and the DHS Privacy Compliance Process

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

This is the DHS Privacy Office's ninth comprehensive report to Congress on DHS activities that involve data mining and the seventh report pursuant to the Federal Agency Data Mining Report Act of 2007 (Data Mining Reporting Act).[14] The Homeland Security Act expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[15] DHS exercises this authority to engage in data mining in the programs discussed in this report, all of which have been reviewed by the Chief Privacy Officer for potential impacts on privacy. The DHS Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974, as amended (Privacy Act);[16] the E-Government Act of 2002 (E-Government Act);[17] and Section 222 of the Homeland Security Act, which states that the DHS Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustain[s], 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.

[13] 6 U.S.C. § 142. The authorities and responsibilities of the Chief Privacy Officer were last amended by the 9/11 Commission Act on August 3, 2007. The 9/11 Commission Act added investigative authority, the power to issue subpoenas to non-Federal entities, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under Section 222 of the Homeland Security Act. These responsibilities are further described on the DHS Privacy Office website (http://www.dhs.gov/privacy) and in the *DHS Privacy Office 2014 Annual Report to Congress*, available at http://www.dhs.gov/sites/default/files/publications/dhs-privacy-office-2014-annual-report-FINAL.pdf.

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

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

[16] 5 U.S.C. § 552a.

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

[18] 6 U.S.C. § 142(a)(1).

The DHS Privacy Office's privacy compliance policies and procedures are based on the Fair Information Practice Principles (FIPPs), which are rooted in the tenets of the Privacy Act. The FIPPs have served as DHS's core privacy framework since the Department was established. They are memorialized in the Privacy Office's *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*[19] and in Department-wide directives including, most recently, Directive 047-01, *Privacy Policy and Compliance* (July 7, 2011).[20] The FIPPs govern the appropriate use of Personally Identifiable Information (PII) at the Department. DHS uses the FIPPs to enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it fulfills the Department's mission to preserve, protect, and secure the homeland. The Office applies the FIPPs to the full breadth and diversity of Department systems and programs that use PII, including DHS activities that involve data mining.

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

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

[19] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[20] Directive 047-01 and its accompanying Instruction are available at https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf and https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-instruction-047-01-001.pdf, respectively. The Directive supersedes the DHS Directive 0470.2, *Privacy Act Compliance*, which was issued in October 2005.

[21] The E-Government Act mandates PIAs for all federal agencies when there are new electronic collections of, or new technologies applied to, PII. Pub. L. No. 107-347. As a matter of policy, DHS extends this requirement to all programs, systems, and activities that involve PII or are otherwise privacy-sensitive.

[22] The Privacy Act requires federal agencies to publish SORNs for any group of records under agency control from which information is retrieved by the name of an individual or by an identifying number, symbol, or other identifier assigned to the individual. 5 U.S.C. § 552a(a)(5) and (e)(4).

regarding how information is used, retained, and may be accessed or corrected. Part of the Privacy Act analysis requires determining whether to apply certain Privacy Act exemptions to limit access to records by an individual for law enforcement or national security reasons. If a SORN is required, the program manager works with the Component privacy officer or PPOC and Component counsel to write a SORN and submits it to the DHS Privacy Office Compliance Group for review and approval by the Chief Privacy Officer.

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

After privacy compliance documentation has been completed and a program, system, or initiative is operational, the DHS Privacy Office also has the authority to monitor and verify ongoing compliance through a Privacy Compliance Review (PCR) conducted by the Office's Oversight Group. Consistent with the Office's unique role as both an advisory and an oversight body for the Department's privacy-sensitive programs and systems, the PCR is designed as a constructive mechanism for improving compliance with assurances made in existing PIAs, SORNs, or Information Sharing Access Agreements or similar agreements. Department PIAs increasingly include a PCR requirement, to demonstrate the Department's commitment to ongoing monitoring of privacy compliance. For example, U.S. Customs and Border Protection (CBP) and the Privacy Office issued a PIA for CBP's Analytical Framework for Intelligence (AFI), discussed below in Section IV.B of this report, which requires that a PCR be completed within 12 months of AFI's deployment. The Privacy Office published the AFI PCR on December 19, 2014, which contains a number of recommendations.[24]

The DHS Privacy Office identifies DHS programs that engage in data mining through several processes in addition to its routine compliance oversight activities. The Office reviews all of the Department's Exhibit 300 budget submissions to the Office of Management and Budget (OMB) to learn of programs or systems that use PII and to determine whether they address privacy appropriately.[25] The Office uses the PTA to review all information technology systems that are going through the security authorization process required by the Federal Information Security Management Act of 2002 (FISMA)[26] to determine whether they maintain PII. The PIA process also provides the Office insight into technologies used or intended to be used by DHS. These oversight activities provide the Office opportunities to learn about proposed data mining activities and to engage program managers in discussions about potential privacy issues.

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

[24] The AFI PCR is available at http://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.

[25] The DHS Privacy Office Compliance Group reviews all major DHS IT programs 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.

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

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

III. Reporting: Program Updates

In the 2013 DHS Data Mining Report,[27] the DHS Privacy Office discussed the following Department programs that engage in data mining, as defined by the Data Mining Reporting Act:

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

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

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

(4) The FALCON-Roadrunner system, which is administered by ICE; and

(5) The DHS Data Framework, which is a DHS-wide initiative.

This section of the 2014 report presents complete descriptions of these programs together with updates on modifications, additions, and other developments that have occurred in the current reporting year, including use of ATS by DHS components other than CBP.

A. Automated Targeting System (ATS)

1. 2014 Program Update

a) Non-Immigrant and Immigrant Visa Applications

As described in the 2012 PIA,[28] ATS-P (now known as ATS-UPAX) is used to vet non-immigrant visa applications for the U.S. Department of State (DoS). In January 2013, CBP and DoS began pre-adjudication investigative screening and vetting for immigrant visas. DoS sends online visa application data to ATS-UPAX for pre-adjudication investigative screening. ATS-UPAX vets the visa application and provides a response to the DoS's Consular Consolidated Database (CCD)[29] indicating whether DHS has identified derogatory information about the individual. Applications of individuals for whom derogatory information is identified through ATS-UPAX are either vetted directly in ATS-UPAX if a disposition can be determined without further investigation or additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net) case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD. The Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA) (Pub. L. 107-173), specifically

[27] http://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf.
[28] The ATS PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.
[29] The CCD PIA *is* available at http://www.state.gov/documents/organization/93772.pdf.

8 U.S.C. § 1721, authorizes the use of ATS-UPAX for screening non-immigrant and immigrant visas.

b) Overstay Vetting

In July 2014, Phase 3 of the One DHS Overstay Vetting effort went live, transitioning from a pilot project to operational status. Overstay Vetting employs the Overstay Hotlist, a list of overstay leads derived from data obtained through ATS, to develop priorities based on associated risk patterns related to national security and public safety. This prioritized list of overstay leads is then passed on to ICE's LeadTrac[30] system for further investigation and possible enforcement action. In addition to prioritizing overstay leads, ATS is also used to vet overstay candidates received from the Arrival and Departure Information System (ADIS)[31] to identify potential additional information on visa overstay candidates based on supporting data available through ATS, i.e., border crossing information (BCI), Form I-94 Notice of Arrival/Departure records, and data from the DHS Student Exchange Visitor Information System (SEVIS).[32]

As with the Phase 2 Pilot, discussed in the 2013 Data Mining Report,[33] Phase 3 also uses foreign national overstay data obtained through system processing in ATS-UPAX and ADIS to identify certain individuals who have remained in the United States beyond their authorized period of admission (overstays) and who may present a heightened security risk. The Department implemented its long term solution during the course of this reporting year. In January 2014, ADIS transitioned from the Office of Biometric Identity Management (OBIM) in the DHS National Protection and Programs Directorate to CBP.[34] The goal of the Overstay Vetting effort is to allow ICE to deploy its investigative resources efficiently to locate high-risk overstays and initiate criminal investigations or removal proceedings against those individuals. CBP uses biographical information on identified and possible overstays in ADIS to be run in ATS-UPAX against risk-based rules based on information derived from past investigations and intelligence. CBP provides results of these analyses from ADIS to ICE for further processing. These

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

[31] The PIA for ADIS is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf, and the SORN for ADIS is available at http://www.gpo.gov/fdsys/pkg/FR-2013-05-28/html/2013-12390.htm. The PIA Update for ATS at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf and the DHS/ALL PIA for the Overstay Vetting Pilot at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_odovp.pdf also address this activity.

[32] The PIA for SEVIS is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis_update_nctc.pdf, and the SORN for SEVIS is *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm.

[33] 2013 Data Mining Report at p. 11.

[34] *See* Consolidated Appropriations Act, 2014, Pub. L. No. 113-76 (Jan. 17, 2014).

activities are covered by PIAs for ATS[35] and the US-VISIT Technical Reconciliation Analysis Classification System[36] and Overstay Vetting.[37]

The legal authorities for the One DHS Overstay Vetting Pilot include: the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000, Public Law 106–215; the Visa Waiver Permanent Program Act of 2000, Public Law 106–396; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Public Law 107–56; EBSVERA; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53.[38]

2. Special ATS Programs

a) ATS Enhancements to Watchkeeper System

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

USCG enhanced Watchkeeper by integrating the ATS-N and ATS-UPAX modules, discussed below, as tools to conduct pre-arrival screening and vetting of vessel cargo, crew, and passengers, and moved the program to operational status in November 2014. The ATS-enhanced Watchkeeper provides near real-time data for Captains of the Port (COTP) to better evaluate threats and deploy resources through the active collection of incoming vessel information. With a more detailed picture of the risk profile that a vessel presents, COTPs can make appropriate, informed decisions well ahead of the vessel's arrival in port. USCG legal authorities for the ATS-Enhanced Watchkeeper system include the Security and Accountability for Every Port (SAFE Port) Act of 2006, 46 U.S.C. § 70107A; 5 U.S.C. § 301; 14 U.S.C. § 632; 33 U.S.C. §§ 1223, 1226; 46 U.S.C. §§ 3717, 12501; Section 102 of the Maritime Transportation Security Act of 2002, Pub. L. No. 108-274; Section 102(c) of the Homeland Security Act, 14 U.S.C. § 2; 33 C.F.R. part 160; and 36 C.F.R. chapter XII. The DHS Privacy Office and USCG published a PIA for Watchkeeper on January 4, 2013.[39]

[35] *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

[36] *See* DHS/NPPD/USVISIT/PIA-004 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_tracs.pdf. CBP will update the ATS and ADIS PIAs to reflect the move of ADIS from OBIM to CBP.

[37] The DHS Overstay Vetting Pilot PIA was issued on December 29, 2011, to add another layer of analysis to this process that can be updated as the program matures. The PIA lists all of the SORNs applicable to this program and is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_odovp.pdf.

[38] A complete list of authorities is included in the PIA for the Overstay Vetting Pilot.

[39] http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_uscg_watchkeeper_20130104.pdf.

b) Secure Flight

In January 2014, CBP and the Transportation Security Administration (TSA) began the initial phase of an effort to improve the vetting of travelers through the leveraging of common procedures, technology, and information sharing between the components. This new effort is called the TSA/CBP Common Operating Picture (COP) Program. The first phase of this program involved the creation of a COP, a single unclassified location, where all travel of Inhibited Passengers (persons identified as matches to the Centers for Disease Control and Prevention Do Not Board List (DNBL), the No Fly and Selectee subsets of the Terrorist Screening Center (TSC) Terrorist Screening Database (TSDB), or who are traveling companions of these travelers) discovered by TSA and CBP is displayed to both components. TSA shares Secure Flight information regarding persons it identifies as Inhibited Passengers through its normal vetting procedures with CBP through TSA's Operations Center's incident management system. CBP stores the information in ATS-UPAX and displays the TSA-identified Inhibited Passengers alongside CBP-identified Inhibited Passengers on a read-only common dashboard display at CBP's National Targeting Center (NTC) and TSA's Operations Center. Joint display of Inhibited Passenger information permits both TSA and CBP to identify and resolve discrepancies in vetting members of the traveling public. CBP published a PIA Update to ATS on January 31, 2014, discussing these efforts.[40]

Following the success of Phase 1 of this program, TSA and CBP sought to move beyond their success in resolving vetting inconsistencies of watchlisted passengers to expand their collective view of air domain security. Phase 2 of the TSA/CBP COP program began in September 2014, and seeks to expand the success of Phase 1 by including additional information in the common dashboard display for both TSA and CBP. This information will include: passengers who are confirmed or possible matches to the watchlists on international flights of covered U.S. aircraft operators; passengers on domestic flights who are confirmed matches to the DNBL or TSDB watchlists; passengers who possess certain derogatory holdings that warrant enhanced scrutiny; and travelers with a high probability of being denied boarding by an aircraft operator on a carrier bound for or departing the United States. CBP published a PIA Update to ATS on September 16, 2014, further discussing these implemented enhancements.[41]

These enhancements build upon the information sharing efforts between Secure Flight and ATS discussed in the 2013 report in which DHS noted that Secure Flight leveraged real-time, threat-based intelligence rules run by ATS-UPAX to identify individuals requiring enhanced security screening prior to boarding an aircraft. On the basis of those rules, Secure Flight transmits to the airlines instructions identifying such individuals. More information about Secure Flight is included in the Secure Flight PIA, which was updated most recently on September 4, 2013.[42] An annex to this report containing Sensitive Security Information (SSI) about Secure Flight's use of ATS-UPAX 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 49 U.S.C. § 44903(j)(2)(C).

[40] http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-atsupdate-01312014.pdf.

[41] http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_tsacop_09162014.pdf.

[42] https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf.

c) Air Cargo Advance Screening Pilot

During this reporting period, CBP and TSA continued to conduct the Air Cargo Advance Screening (ACAS) joint pilot discussed in the 2013 Data Mining Report,[43] using existing CBP data collections and ATS-N to identify pre-departure air cargo that may pose a threat to aviation. In July 2014, CBP extended the pilot through July 26, 2015.[44] TSA targeting personnel work side-by-side with CBP targeting personnel jointly to develop rules designed to address threats from air cargo and to review data in ATS. TSA legal authorities for this pilot include 49 U.S.C. § 114(f)(10), which authorizes TSA to ensure the adequacy of security measures for the transportation of cargo, and Section 1602 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), which amended 49 U.S.C. § 44901 to require TSA to provide for the screening of cargo on passenger and all-cargo aircraft.

3. General ATS Program Description

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

ATS consists of five modules that focus on exports,[45] imports, passengers and crew (airline passengers and crew on international flights, and passengers and crew on sea carriers), private vehicles crossing at land borders, and a workspace to support the creation and retention of analytical reports. This report discusses all of these modules: ATS-N and ATS-AT (both of which involve the analysis of cargo), ATS-L (which involves analysis of information about vehicles and their passengers crossing the land border), ATS-UPAX (which involves analysis of information about certain travelers), and the ATS Targeting Framework (ATS-TF) (a platform for temporary and permanent storage of data).

[43] 2013 Data Mining Report at p. 7.

[44] 79 FR 43766 (July 28, 2014), available at https://federalregister.gov/a/2014-17724.

[45] At the time of this report, CBP maintains the export targeting functionality in the Automated Targeting System (ATS). In January 2014, the Automated Export System (AES) was re-engineered onto the ATS IT platform and is covered by the Export Information System (EIS) privacy compliance documentation. CBP has made no changes to the manner in which it targets exports; however, access to this targeting functionality now occurs by logging in through AES. The location of the login to the export targeting functionality in AES is intended to improve efficiency related to user access to export data and its associated targeting rules and results. An update to the EISPIA will discuss these updates involving AES and ATS in greater detail.

The U.S. Customs Service, a legacy organization of CBP, traditionally employed computerized tools to target potentially high-risk cargo entering, exiting, and transiting the United States. ATS was originally designed as a rules-based program to identify such cargo; it did not apply to travelers. ATS-N and ATS-AT[46] became operational in 1997. ATS-P (now known as ATS-UPAX)[47] became operational in 1999 and is now critical to CBP's mission. ATS-UPAX allows CBP officers to determine whether a variety of potential risk indicators exist for travelers or their itineraries that may warrant additional scrutiny. ATS-UPAX maintains Passenger Name Record (PNR) data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from certain air carriers in 1997. Currently, CBP collects this information to the extent it is collected by carriers in connection with a flight into or out of the United States, as part of CBP's border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).[48]

ATS ingests various data in real-time from the following DHS and CBP systems: the Automated Commercial System (ACS), the Automated Manifest System (AMS), the Advance Passenger Information System (APIS), the Automated Export System (AES), the Automated Commercial Environment (ACE), the Electronic System for Travel Authorization (ESTA), the Nonimmigrant Information System (NIIS), DHS BCI, ICE's SEVIS, and TECS.[49] TECS includes information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[50] TSDB and provides access to the Department of Justice's (DOJ) National Crime Information Center (NCIC), which contains information about individuals with outstanding wants and warrants, and to Nlets (formerly the National Law Enforcement Telecommunications System), a clearinghouse for state wants and warrants as well as information from state Departments of Motor Vehicles (DMV). ATS collects PNR data directly from air carriers. ATS also collects data from certain airlines, air cargo consolidators (freight forwarders), and express consignment services in ATS-N. ATS accesses data from these sources, which collectively include: electronically filed bills of lading (i.e., forms provided by carriers to confirm the receipt and transportation of on-boarded cargo to U.S. ports), entries, and entry summaries for cargo imports; Electronic Export Information (EEI) (formerly referred to as Shippers' Export Declarations) submitted to AES and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land border crossing and referral records for vehicles crossing the border; airline reservation data; non-immigrant entry records; records from secondary referrals, incident logs, and suspect and violator indices; seizures; and information from the TSDB and other government databases regarding individuals with outstanding wants and warrants and other high-risk entities.

[46] Functionality of ATS-AT was modernized when the AES system was recently re-engineered and deployed by CBP.

[47] ATS-UPAX is an updated user interface that replaced the older functionality of ATS-P.

[48] 49 U.S.C. § 44909. The regulations implementing ATSA are codified at 19 C.F.R. § 122.49d.

[49] PIAs for these programs can be found at www.dhs.gov/privacy.

[50] The TSC is an entity established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the FBI, established the TSC pursuant to Homeland Security Presidential Directive 6, which required the Attorney General to establish an organization to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening and law enforcement processes. The TSC maintains the Federal Government's consolidated terrorist watch list, known as the TSDB.

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

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

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

i. Program Description

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

The functionality of ATS-AT was modernized when the AES system was recently re-engineered and deployed by CBP. AES 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. This targeting functionality in AES sorts EEI data, compares it to a set of rules, and evaluates it in a comprehensive fashion. This information assists CBP officers in targeting or identifying exports that pose potential aviation safety and security risks (e.g., hazardous materials) or may be otherwise exported in violation of U.S. law.

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

ii. Technology and Methodology

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

The SAFE Port Act requires ATS to use or investigate the use of advanced algorithms in support of its mission.[51] To that end, as discussed in previous DHS Data Mining Reports, ATS established an Advanced Targeting Initiative, which employs the development of data mining, machine learning,[52] and other analytic techniques to enhance ATS-N and ATS-AT. This Initiative strives to improve law enforcement capabilities with predictive models and establish performance evaluation measures to assess the effectiveness of ATS screening for inbound and outbound cargo shipments across multimodal conveyances.

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

The Advanced Targeting Initiative is part of ATS's maintenance and operation of the ATS-N and ATS-AT. The design and tool-selection processes for data mining, pattern recognition, and machine learning techniques under development in the Advanced Targeting Initiative are being evaluated through user acceptance testing by the National Targeting Center-Cargo (NTC-C). The NTC-C and CBP Office of Intelligence and Investigative Liaison further support the performance of research on entities and individuals of interest, data queries, data manipulation on large and complex datasets, data management, link analysis, social network analysis,[53] and statistical analysis in support of law enforcement and intelligence operations. Upon successful testing, the programming enhancements are included in maintenance and design updates to system operations and deployed at the national level to provide a more uniform enhancement to CBP operations. This practice will continue to be incorporated into future maintenance protocols for ATS.

iii. Data Sources

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

[51] 6 U.S.C. § 901.

[52] 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.

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

ATS-N and ATS-AT use the information from source databases to gather information about importers and exporters, cargo, and conveyances used to facilitate the importation of cargo into and the exportation of cargo out of the United States. This information includes PII concerning individuals associated with imported and exported cargo (e.g., brokers, carriers, shippers, buyers, sellers, exporters, freight forwarders, and crew). ATS-N receives data pertaining to entries and manifests from ACS and ACE, and processes it against a variety of rules to make a rapid, automated assessment of the risk of each import.[54] ATS-AT uses EEI data that exporters file electronically with AES, export manifest data from AES, and export airway bills of lading to assist in formulating risk assessments for cargo bound for destinations outside the United States.

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

iv. Efficacy

Based on 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.

In the past year, CBP officers working at the NTC-C have used ATS-N to identify, through risk-based rule sets, cargo shipments and commodities that were matches to criteria contained in the rule, which caused these shipments to be referred for further examination. CBP officers apply additional scrutiny to such referrals; including opening the cargo container to remove and inspect its contents. During the exam, CBP officers will seize and forfeit, or detain, subject to re-exportation, commodities that are contraband or otherwise not admissible. For example, CBP officers working at the NTC-C used the Ag/Bio-terrorism rule sets (ABTC2) to identify a shipment whose commodity was listed as “Pharmaceuticals.” NTC-C contacted CBP personnel at the CBP Louisville United Parcel Service Hub to request an inspection of the shipment for prohibited pharmaceuticals. In November 2014, the shipment was examined and seized because it contained 90 Vyvanse pills (an amphetamine and Schedule II controlled substance). In another example, NTC-C employed ABTC2 to conduct research on a shipment, whose commodity was listed as “Botox PDR.” Using the targeting results, officers at NTC-C contacted CBP personnel at the John F. Kennedy Mail Facility to request an examination because the shipper had been linked to sending restricted pharmaceuticals to consignees who were not registered importers with the Food and Drug Administration (FDA). Upon confirmation of the contents of the mail

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

package, the shipment was detained in March 2014, and transferred to FDA for re-exportation and disposition in accordance with FDA's authorities.

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.[55] ATS-AT and ATS-N also support functions mandated by Title VII of Public Law 104-208 (Omnibus Consolidated Appropriations Act, 1997), which provides funding for counterterrorism and drug law enforcement. ATS-AT also supports functions arising from the Anti-Terrorism Act of 1987[56] and the 1996 Clinger-Cohen Act.[57] The risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.[58]

b) ATS-Unified Passenger Module (ATS-UPAX, formerly ATS-P)

i. Program Description

ATS-UPAX is a custom-designed system used at U.S. ports of entry, particularly those receiving international flights and voyages (both commercial and private), and the CBP NTC to evaluate passengers and crew members prior to their arrival to or departure from the United States. ATS-UPAX was deployed as an update to the ATS-P functional interface in March 2013. ATS-UPAX facilitates the CBP officer's decision-making process about whether a passenger or crew member should receive additional inspection prior to entry into, or departure from, the country because that person may pose a greater risk for terrorism and related crimes or other crimes. ATS-UPAX is a fully operational application that utilizes CBP's System Engineering Life Cycle methodology[59] and is subject to recurring systems maintenance.

ii. Technology and Methodology

ATS-UPAX is an updated user interface that replaces the older functionality of the ATS-P interface to process traveler information against other information available in ATS, and apply 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 updates to ATS that comprise ATS-UPAX involve a cleaner visual presentation of relevant information used in the screening process. This presentation involves providing direct access to cross-referenced files and information from partner agency databases through the use of hypertext links and single sign-on protocols. The

[55] *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.
[56] 22 U.S.C. § 5201 *et seq.*
[57] 40 U.S.C. § 1401 *et seq.*
[58] 6 U.S.C. § 912(b).
[59] CBP's Office of Information & Technology's System Engineering Life Cycle (SELC) is a policy that lays out the documentation requirements for all CBP information technology projects, pilots, and prototypes. All projects and system changes must have disciplined engineering techniques, such as defined requirements, adequate documentation, quality assurance, and senior management approvals, before moving to the next stage of the life cycle. The SELC has seven stages: initiation and authorization, project definition, system design, construction, acceptance and readiness, operations, and retirement.

links and sign-on protocols employ the underlying sharing agreements that support the prior information query capability within the former ATS-P to permit a more seamless integration, allowing relevant data to be consolidated or accessed from the primary screen used to vet the targeting results pertaining to the traveler.

ATS-UPAX continues to rely on the risk-based rules that 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-UPAX does not use a score to determine an individual's risk level; instead, ATS-UPAX compares information in ATS source databases against watch lists, criminal records, warrants, and patterns of suspicious activity identified through past investigations and intelligence. The results of these comparisons are either assessments of the risk-based rules that a traveler has matched or matches against watch lists, criminal records, or warrants. The rules are run against continuously updated incoming information about travelers (e.g., information in passenger and crew manifests) from the data sources listed below. While the rules are initially created based on information derived from past investigations and intelligence, data mining queries of data in ATS and its source databases may subsequently be used by analysts to refine or further focus those rules to improve the effectiveness of their application.

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

iii. Data Sources

ATS-UPAX uses available information from the following databases to assist in the development of the risk-based rules discussed above. ATS-UPAX vetting relies upon information in APIS; NIIS, which contains all Form I-94 Notice of Arrival/Departure records and actual ESTA arrivals/departures; ESTA, which contains pre-arrival information for persons traveling from Visa Waiver Program (VWP)[60] countries; the DHS Suspect and Violator Indices (SAVI); and the Department of State visa databases. ATS-UPAX also relies upon PNR information from air

[60] 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 (INA), 8 U.S.C. § 1187, and 8 C.F.R. part 217. Section 711 of the 9/11 Commission Act amended Section 217 to strengthen the security of the VWP. ESTA is an outgrowth of that mandate. More information about ESTA is available at http://www.cbp.gov/esta.

carriers, BCI crossing data, seizure data, Report of International Transportation of Currency or Monetary Instrument Form (CMIR) data,[61] and information from the TSDB and TECS.

iv. Efficacy

ATS-UPAX provides information to its users in near real-time. The flexibility of ATS-UPAX'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-UPAX greatly increases the efficiency and effectiveness of the officers' otherwise manual and labor-intensive work checking separate databases, thereby facilitating the more efficient movement of travelers while safeguarding the border and the security of the United States. CBP officers use the information generated by ATS-UPAX to aid their decision-making about the risk associated with individuals. As discussed below, ATS includes real-time updates of information from ATS source systems to ensure that CBP officers are acting upon accurate information.

In the past year, ATS-UPAX has identified, through lookouts and/or risk-based rule sets, individuals who were confirmed matches to the TSDB and caused action to be taken to subject them to further inspection or, in some cases, took action to prevent them from boarding. ATS-UPAX matches have also enabled CBP officers and foreign law enforcement partners to disrupt and apprehend persons engaged in human trafficking and drug smuggling operations. For example, CBP officers working at the NTC using ATS-UPAX identified a traveler as a possible match to an ATS risk assessment, categorizing him as a possible affiliate of a person listed in the TSDB. NTC referred the traveler to CBP officers at the Vancouver Preclearance Station where secondary inspection confirmed the link, which resulted in the denial of the traveler's admission to the United States. In another instance, CBP officers using ATS-UPAX employed a rule referred to as "Operation Rubix Cube" and identified a passenger from Lagos, Nigeria, who during secondary inspection and a subsequent x-ray exam was found to be smuggling 3.39 pounds of heroin in her body.

Finally, a traveler departing Qatar and intending to travel to Washington, D.C. was referred to Immigration Advisory Program (IAP) personnel[62] by officers using ATS-UPAX to assess the traveler's risk. During a review of the traveler's documents[63] and an interview, the traveler struggled to answer basic questions regarding his status in the U.S. Subsequent research through ATS revealed that the person associated with the documents (later determined to be his brother) had become a citizen a month earlier. A photo comparison from the new citizen's U.S. passport confirmed the false identity resulting in a recommendation to the airline that the traveler be denied boarding. Further research in ATS-UPAX also confirmed that the U.S. citizen (brother)

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

[62] CBP IAP personnel are posted at the host country's airport during processing of flights bound for the United States. These unarmed, plain-clothes officers assist airline and security employees with the review of traveler information during the processing of U.S.-bound flights to identify potential threats and assist partner countries in reducing the number of improperly documented travelers. *See* Immigration Advisory Program Fact Sheet available at http://www.cbp.gov/sites/default/files/documents/immig_advis_prog_2.pdf.

[63] Passport with an Alien Documentation and Identification Telecommunication (ADIT) stamp supporting a claim of Lawful Permanent Resident (LPR) status.

had traveled to Qatar with the traveler; he was identified to Qatari security officials for questioning.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.[64] As part of this inspection and examination process, each traveler seeking to enter the United States must first establish his or her identity, nationality, and, when appropriate, admissibility to the satisfaction of the CBP officer and then submit to inspection for customs purposes. The information collected is authorized pursuant to the EBSVERA,[65] ATSA, Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the INA, and the Tariff Act of 1930, as amended.[66] Much of the information collected in advance of arrival or departure can be found on routine travel documents that passengers and crew members may be required to present to a CBP officer upon arrival in or departure from the United States.

c) ATS-Land Module (ATS-L)

i. Program Description

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

ii. Technology and Methodology

ATS-L processes vehicle, vehicle occupant, and pedestrian information against other data available to ATS, and applies rules developed by subject matter experts (officers and agents drawing upon years of experience reviewing historical trends and current threat assessments), system learning rules (rules resulting from the system's weighting positive and negative results from subject matter expert rules), or affiliate rules (derived from data establishing an association with a known violator). System learning rules in ATS-L seek to identify high-risk vehicles by examining historical trends in CBP narcotics seizure record data from the land ports of entry. These rules are driven by algorithms to identify obvious and non-obvious relationships among data inputs (i.e., reviewing historical seizure data and applying trend analysis to incoming vehicle and traveler data). The system learning rules are being updated through the use of a new predictive model to help identify personal vehicles with an increased risk of transporting certain

[64] *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.
[65] Pub. L. No. 107-173.
[66] 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.

types of illegal drugs; completion of the new model roll-out to the entire southwest border occurred in May 2014. The subject matter expert rules, which are designed by CBP personnel to create scenarios based on officer experience and law enforcement or intelligence information, are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. ATS-L also compares license plate and DMV data to information in ATS source databases including watch lists, criminal records, warrants, and a statistical analysis of past crossing activity. The results of these comparisons are either assessments recommending further official interest in a vehicle and its occupants or supporting information for the clearance and admission of the vehicle and its occupants.

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

iii. Data Sources

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

iv. Efficacy

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

v. Laws and Regulations

CBP is responsible for collecting and reviewing information about vehicles and their occupants prior to entering the United States.[67] As part of this inspection and examination process, the occupants of each vehicle seeking to enter the United States must first establish their identity, nationality, and, when appropriate, admissibility to the satisfaction of the CBP officer and must submit to inspection for customs purposes. Information collection in ATS-L is pursuant to the authorities for information collection in ATS-UPAX (i.e., EBSVERA; ATSA; IRTPA; the INA, and the Tariff Act of 1930, as amended). Much of the information collected in advance of or at the time of arrival can be found on routine travel documents possessed by the occupants (which they may be required to present to a CBP officer upon arrival in the United States), the vehicle's license plate, and official records pertaining to the registry of the vehicle.

4. ATS Privacy Impacts and Privacy Protections

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

Authorized CBP officers and personnel from ICE, TSA, USCG, 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.[68] 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 on 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.

Additional ATS users include federal agencies with authority governing the safety of products imported into the United States, or with border management authorities, who have joined with DHS (through CBP, and in coordination with ICE) to form the Import Safety Commercial Targeting and Analysis Center (CTAC) in Washington, D.C. to promote the need to share information about the safety of those products. These agencies include: the U.S. Consumer Product Safety Commission, the Food Safety Inspection Service, the Animal Plant Health Inspection Service, the Pipeline and Hazardous Materials Safety Administration, the National Highway Traffic Safety Administration, Environmental Protection Agency, FDA, U.S. Fish and Wildlife Service, and the National Marine Fisheries Service. Each member of the CTAC

[67] *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.

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

provides representatives who are assigned to work at the CTAC to collaborate and cooperate on issues relating to cargo enforcement and import safety.

ATS relies upon its source systems to ensure the accuracy and completeness of the data they provide to ATS. When a CBP officer identifies any discrepancy regarding the data, the officer will take action to correct that information, when appropriate. ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real time, or near-real time, from TECS, which includes data accessed from NCIC and Nlets, as well as from ACE, AMS, ACS, AES, ESTA, NIIS, BCI, SEVIS, and APIS. When corrections are made to data in source systems, ATS updates this information in near-real time and uses the latest data. In this way, ATS integrates all updated data (including accuracy updates) in as close to real time as possible.[69]

In the event that PII (such as certain data within a PNR) used by or maintained in ATS-UPAX is believed by the data subject to be inaccurate, the subject has access to the redress process previously developed by DHS. The individual is provided information about this process during examination at secondary inspection. CBP officers have a brochure available to each individual entering and departing the United States that provides CBP's Pledge to Travelers. This pledge gives each traveler an opportunity to speak with a passenger service representative to answer any questions about CBP procedures, requirements, policies, or complaints.[70] CBP has created the CBP INFO Center in its Office of Public Affairs to serve as a clearinghouse for all redress requests, that come to CBP directly and concern inaccurate information collected or maintained by its electronic systems, including ATS. This process is available even though ATS does not form the sole basis for identifying enforcement targets. To facilitate the redress process, DHS has created a comprehensive, Department-wide program, the Traveler Redress Inquiry Program (DHS TRIP), to receive all traveler-related comments, complaints, and redress requests affecting its component agencies. Through DHS TRIP, travelers can seek resolution regarding difficulties they experienced during their travel screening and inspection.[71]

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

[69] 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.
[70] The Pledge is available at http://www.cbp.gov/travel/customer-service/cbp-pledge-to-travelers. In addition, travelers can visit CBP’s INFO Center website at http://www.cbp.gov/travel/customer-service to request answers to questions and submit complaints electronically. This website also provides travelers with the address of the CBP INFO Center and the telephone number of the Joint Intake Center.
[71] DHS TRIP can be accessed at http://www.tsa.gov/traveler-information/dhs-traveler-redress-inquiry-program-dhs-trip.

of access to PII held in source systems.[72] Privacy Act and FOIA requests for access to information for which ATS is the source system are directed to CBP.[73]

ATS underwent the Security Authorization process in accordance with DHS and CBP policy and obtained its initial Security Authorization on June 16, 2006. ATS also completed a Security Risk Assessment on March 28, 2006, in compliance with FISMA, OMB policy, and National Institute of Standards and Technology guidance. The ATS Security Authorization and Security Risk Assessment were subsequently updated and are valid until January 30, 2017.

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

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

The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be disposed of in accordance with ATS's National Archives and Records Administration (NARA)-approved record retention schedule, except as noted below.[74] The retention period for PNR, which is contained only in ATS-UPAX, will be subject to the following further access restrictions and masking requirements: ATS-UPAX users with PNR access will have access to PNR in an active database for up to five years, with the PNR depersonalized and masked after the first six months of this period. After the initial five-year retention period in the active database, the PNR will be transferred to a dormant database for a period of up to ten years. PNR in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be unmasked in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk.[75]

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

[72] 5 U.S.C. § 552.

[73] Requests may be submitted by mail to FOIA Division, 90 K Street NE, Washington, DC 20229-1181.

[74] NARA approved the record retention schedule for ATS on April 12, 2008.

[75] These masking requirements have been implemented pursuant to the 2011 U.S.-European Union PNR Agreement entered into force on June 1, 2012. The Agreement is available on the Privacy Office website at http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.

accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

B. Analytical Framework for Intelligence (AFI)

1. 2014 Program Update

The 2013 Data Mining Report described how AFI became the user interface for access to select datasets that formerly resided in ICE's Intelligence Fusion System (IFS) as discussed below in section IV.B.4.[76] As a result, AFI now provides federated access to these datasets for ICE analysts.

AFI continued the Cross Domain Capabilities (CDC) program pilot in 2014, which enables analysts to view both Secret and Sensitive But Unclassified (SBU) data on the same screens. Previously, all DHS data sources utilized in AFI had been unclassified. Under the CDC Pilot, user login information is collected as part of a cross domain guard[77] audit function to ensure security and information handling procedures. PII from AFI is transmitted through the guard from SBU to secret domains. The guard neither stores, generates, nor retains PII. The CDC Pilot allows more effective information flow between security domains, but does not allow the collection, retention or storage of any data other than user access information.

The CDC Pilot, and the addition of select legacy IFS datasets to AFI, will be included in a PIA update for AFI to be completed after the Privacy Office's PCR of AFI, which was published on December 19, 2014.[78]

2. Program Description

AFI enhances CBP's ability to identify and apprehend individuals who pose a potential law enforcement or security risk, and aids in the enforcement and prosecution of customs and immigration laws, and other laws enforced by CBP at the border. AFI is used for the purposes of: (1) identifying individuals, associations, or relationships that may pose a potential law enforcement or security risk, targeting cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law; (2) conducting additional research on persons or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and (3) sharing finished intelligence products[79] developed in connection with the above purposes with DHS employees who have a need to know in the performance of their

[76] The PIA for AFI is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf. The AFI SORN is available at http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm and in the Federal Register at 77 FR 33753 (June 7, 2012).

[77] A guard protects the integrity of each system, enabling the movement of unclassified information to a classified system.

[78] The AFI PCR is available at http://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.

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

official duties and who have appropriate clearances or permissions, or externally pursuant to routine uses in the AFI SORN.

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

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

AFI provides a set of analytic tools that include advanced search capabilities into existing DHS sources, and federated queries to other federal agency sources and commercial data aggregators, to allow analysts to search several databases simultaneously. AFI tools scan the query results, associate and extract similar themes, and present the results to the AFI analyst in a manner that allows for easy visualization and analysis.

AFI creates an index of the relevant data in existing operational DHS source systems by ingesting this data from source data systems, as described below, in order to enable a faster return of search results. AFI also permits AFI analysts to upload, index, and store information that may be relevant from other sources, such as the Internet or traditional news media, subject to the procedures described below. Requests for Information (RFI), responses to RFIs, finished intelligence products, and unfinished "projects"[80] are also part of the index. The indexing engines refresh data from the originating system periodically depending on the source data system. AFI adheres to the records retention policies of the source data systems along with their user access controls.

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

AFI also enables analysts to perform federated queries against external data sources, including certain data sets belonging to the Department of State, DOJ/FBI, and commercial data

[80] AFI analysts create "projects" within the AFI workspace to capture research and analysis that is in progress and may or may not lead to a finished intelligence product or RFI response.

aggregators that are already available to DHS users. AFI tracks where AFI analysts search and routinely audits these records. AFI analysts use data that is available from commercial data aggregators to complement or clarify the data to which they have access within DHS. AFI provides a suite of tools that assist analysts in detecting trends, patterns, and emerging threats, and in identifying non-obvious relationships, using the information maintained in the index and made accessible through the federated query.

AFI also serves as a workspace that allows AFI analysts to create finished intelligence products, to maintain and track projects throughout their lifecycle from inception to finished intelligence product or from RFI to response, and to share finished intelligence products either within DHS or externally through regular law enforcement and intelligence channels to authorized users with a need to know, pursuant to routine uses in the AFI SORN.[81]

3. Technology and Methodology

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

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

Specific types of analysis include:

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

[81] A detailed description of the processes leading to finished intelligence products and RFI responses is included in the PIA for AFI.

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

4. Data Sources

The AFI system does not itself collect information directly from individuals. Rather, AFI performs searches for and accesses information collected and maintained in other systems, including information from both government-owned sources and commercial data aggregators. If, however, a particular data source is not available due to technical issues, the AFI analyst will be unable to retrieve the responsive record in its entirety. Additionally, AFI analysts may upload information that they determine is relevant to a project, including information publicly available on the Internet.

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

- *DHS-Owned Data that AFI automatically collects and stores*: This selected data is indexed and then as information is retrieved via a search, data from multiple sources may be joined to create a more complete representation of an event or concept. For example, a complex event such as a seizure that is represented by multiple records may be composed into a single object for display. AFI receives records through:
    - ATS (including: APIS; ESTA; TECS Incident Report Logs and Search, Arrest, Seizure Reports, Primary Name Query, Primary Vehicle Query, Secondary Referrals, TECS Intel Documents; and visa data);
    - Enterprise Management Information System-Enterprise Data Warehouse (including: Arrival and Departure Form I-94; CMIR data; apprehension, inadmissibility, and seizure information from the ICE Immigration and Enforcement Operational Records System (ENFORCE); National Security Entry-Exit Program information from ENFORCE; SEVIS information; and seizure information from the Seized Asset and Case Tracking System);
    - the Targeting Framework (case information).
- *DHS-Owned Data to which AFI provides federated access*: This data is a limited set of data owned, stored, and indexed by other DHS components. Through AFI, only a user with an active account in that other DHS system can query and receive results from that system. AFI will store only results that are returned as a function of AFI's audit capabilities. AFI provides this federated access to select legacy IFS datasets. These datasets include the following information: Enforcement Integrated Database detention

data, ICE intelligence information reports, ICE intelligence products, ICE name trace, ICE significant event notification Detention and Removal Leads, and TECS Reports of Investigation).[82]

- *Other Government Agency Data*: AFI obtains imagery data from the National Geospatial-Intelligence Agency and obtains other government agency data to the extent available through ATS, such as identity and biographical information, wants and warrants, DMV data, and data from the TSDB.[83]
- *Commercial Data*: AFI collects identity and imagery data from several commercial data aggregators so that DHS AFI analysts can cross-reference that information with the information contained in DHS-owned systems. Commercial data aggregators include sources available by subscription only (e.g., Thomson Reuters CLEAR) that connect directly to AFI, and do not include information publicly available on the Internet.
- *AFI Analyst-Provided Information*: This includes any information uploaded by an authorized user either as original content or from an *ad hoc* data source such as the Internet or traditional news media. AFI analyst-provided information may include textual data (such as official reports users have seen as part of their duties or segments of a news article), video and audio clips, pictures, or any other information the user determines is relevant. User-submitted RFIs and projects are also stored within AFI, as well as the responses to those requests.
- *AFI Analyst-Created Information*: AFI maintains user-created projects as well as finished intelligence products. Finished intelligence products are made available through AFI to finished intelligence users.
- *Index Information*: As noted above, AFI ingests subsets of data from CBP and DHS systems to create an index of searchable data elements. The index indicates which source system records match the search term used.

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

5. Efficacy

AFI became operational in August 2012, and CBP has sought to deploy AFI to field and headquarters locations to assign officers, agents, and employees user roles and to provide training commensurate with those roles. Ongoing operational use of AFI along the southwest border has shown that AFI provides valuable assistance to ongoing operations. For example, an analytic unit in Texas created a Project within AFI to identify the network of a very violent enforcement group of a notorious Mexican cartel. Using the unique portfolio of systems, as well as the collaboration space within AFI, the unit developed approximately 22 CBP intelligence

[82] ICE and the Privacy Office issued a PIA for IFS on November 17, 2008. The IFS PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_ifs.pdf.

[83] A more complete discussion of other government agency data that may be accessed through ATS can be found in the ATS PIA.

reports, referred a number of subjects to the NTC for further analysis, and initiated a national ATS rule designed to assist in identifying additional high value enforcement targets.

In another instance, an AFI user conducted research and identified a threat to border security after receiving an RFI. The user leveraged the collaborative environment within AFI to share data with peers during the planning cycle and the initial collections operation. The AFI analysis tools were applied to the consolidated data further to refine the location(s) of the illicit communications activity. A finished product detailing the activity was generated and disseminated to a foreign partner, which ultimately led to the dismantlement of the illicit communications infrastructure.

6. Laws and Regulations

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

7. Privacy Impact and Privacy Protections

CBP does not use the information in AFI to make unevaluated automated decisions about individuals. Given the breadth of the data available to AFI users, CBP has built extensive privacy protections into the structure and governance of AFI.[84] AFI does not collect information directly from individuals; AFI source systems are responsible, as appropriate, for providing individuals the opportunity to decline to provide information or to consent to or opt-out of use information. AFI provides the public notice about its use of information through its PIA and SORN.[85]

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

AFI is being designed and developed in an iterative, incremental fashion. CBP has created a governance board to ensure that AFI is built and used in a manner consistent with the Department’s authorities and that information in AFI is used consistent with the purpose for which it was originally collected. The governance board includes representatives from CBP’s Offices of Intelligence and Investigative Liaison, Field Operations, Border Patrol, Air & Marine, Chief Counsel, Internal Affairs, Information Technology, and Privacy and Diversity, who review requested changes to the system on a quarterly basis and determine whether additional input is required. The governance board directs the development of new aspects of AFI, and reviews and approves new or changed uses of AFI, new or updated user types, and new or expanded data to

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

[85] The PIA for AFI is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf. The AFI SORN is available at http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm and in the Federal Register at 77 FR 33753 (June 7, 2012).

be made available in or through AFI. As an added layer of oversight, the DHS Privacy Office published a PCR for AFI on December 19, 2014.[86]

Although AFI indexes information from many different source data systems, each source system maintains control of the data that it originally collected, even though the data is co-located in both the source system and in AFI. Accordingly, only DHS AFI analysts authorized to access the data in a particular source system have access to that same data through AFI.[87] This is accomplished by passing individual user credentials from the originating system or through a previously approved certification process in another system. Finished intelligence product users and DHS AFI analysts have access to finished intelligence products, but only DHS AFI analysts have access to the source data, projects, and analytical tools maintained in AFI. In order to access AFI, all AFI users are required to complete biannual training in privacy awareness and the privacy training required of all CBP employees with access to CBP's law enforcement systems. This training is regularly updated. Users who do not complete this training lose access to all computer systems, including AFI.

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

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

AFI has built-in system controls that identify what particular users are able to view, query, or write, as well as audit functions that are routinely reviewed. AFI uses security and auditing tools to ensure that information is used in accordance with CBP policies and procedures. The security and auditing tools include: *Role-Based Access Control*, which determines a user's authorization to use different functions, capabilities, and classifications of data within AFI, and *Discretionary Access Control*, which determines a user's authorization to access individual groupings of user-

[86] The AFI PCR is available at http://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.

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

provided data. Data are labeled and restricted based on data handling designations for SBU data (e.g., For Official Use Only (FOUO), SSI, Law Enforcement Sensitive (LES)) and based on need to know.

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

As AFI contains sensitive information related to intelligence, counterterrorism, homeland security, and law enforcement programs, activities, and investigations, DHS has exempted AFI from the access and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(j)(2) and (k)(2). For index data and source data, as described in the SORN for AFI, to the extent that a record is exempted in a source system, the exemption will continue to apply. When there is no exemption for giving access to a record in a source system, CBP will provide access to that information maintained in AFI.[88]

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

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

1. 2014 Program Update

In January 2014, ICE migrated the DARTTS system to the ICE Homeland Security Investigations (HSI) FALCON environment and launched FALCON-DARTTS.[89] The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other government applications and systems, with

[88] Notwithstanding the applicable exemptions, CBP reviews all requests for access to records in AFI on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP, and in accordance with procedures published in the applicable SORN. Requests may be submitted to U.S. Customs and Border Protection, Freedom of Information Act (FOIA) Division, 90 K Street NE, Washington, DC 20229-1181. Additional information on submitting FOIA and Privacy Act requests is included in the PIA for AFI at pp. 22-23.

[89] A comprehensive list of changes to, and new features of, FALCON-DARTTS after the migration from legacy DARTTS is included in the Program Update in the 2013 Data Mining Report.

appropriate user access restrictions and robust user auditing controls.[90] FALCON-DARTTS replicates the functionality of and serves the same user-groups as legacy DARTTS. With the deployment of FALCON-DARTTS, the legacy DARTTS system was retired.[91]

ICE published a new PIA for FALCON-DARTTS on January 16, 2014, to address the migration from legacy DARTTS,[92] as well as updated and published the FALCON Search & Analysis (FALCON-SA) Appendix to reflect that specific datasets and analytical results from FALCON-DARTTS are ingested into FALCON-SA (a module within the FALCON environment) for additional analysis and investigation using tools within FALCON-SA.[93] On December 1, 2014, ICE republished the FALCON-DARTTS SORN to include new datasets analyzed by FALCON-DARTTS.[94]

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

2. Program Description

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

FALCON-DARTTS is owned and operated by the HSI 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 smuggling, trafficking counterfeit merchandise, the fraudulent misclassification of merchandise, and the over- or under-valuation of merchandise to conceal the source of illicitly derived proceeds or as the means to earn illicitly derived funds supporting ongoing criminal activity. As part of the investigative process, HSI investigators and analysts must understand the relationships among importers, exporters, and the financing for a set of trade transactions, to determine which transactions are suspicious and warrant investigation. FALCON-DARTTS is designed specifically to make this investigative

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

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

[92] *See* DHS/ICE/PIA-038 FALCON-DARTTS, January 16, 2014, http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falcondartts_january2014_0.pdf.

[93] *See* DHS/ICE/PIA-032a FALCON-SA, January 16, 2014, http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf.

[94] *See* DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, December 1, 2014, http://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm. Datasets analyzed by FALCON-DARTTS not listed in the TTAR SORN at the time the system became operational in January 2014 were restricted from use in the system until the effective date of the updated SORN published in the *Federal Register*.

process more efficient by automating the analysis and identification of anomalies for the investigator.

FALCON-DARTTS allows HSI to perform research and analysis that are not possible in any other ICE system because of the data it analyzes and the level of detail at which the data can be analyzed.[95] FALCON-DARTTS does not seek to predict future behavior or "profile" individuals or entities (i.e., identify individuals or entities that meet a certain pattern of behavior pre-determined to be suspect). Instead, it identifies trade and financial transactions that are statistically anomalous based on user-specified queries. Investigators analyze the anomalous transactions to determine if they are, in fact, suspicious and warrant further investigation. If determined to warrant further investigation, they will gather additional facts, verify the accuracy of the FALCON-DARTTS data, and use their judgment and experience in deciding whether to investigate further. Not all anomalies lead to formal investigations.

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

All ICE HSI, CBP, and foreign users of FALCON-DARTTS are able to access only data that is associated with the user's specific profile and which that user has the legal authority to access. Specifically, only ICE HSI and CBP users are granted access to the law enforcement data, and only ICE HSI users are granted access to the financial data, maintained in FALCON's general data storage environment.[96] In this environment, the data is aggregated with other FALCON data, and user access is controlled through a combination of data tagging, access control lists, and other technologies.

Foreign users of FALCON-DARTTS are authorized to access only trade data, and are not authorized to access the law enforcement, financial data, or *ad hoc* data that resides in the FALCON general data storage environment. The trade data is stored in a "trade data subsystem" that is physically and logically separate from the FALCON general data storage environment and contains different user access requirements than the overarching data storage environment. Trade data is segregated in a separate storage environment due to its high volume and to enhance security controls for foreign users who only access trade data. Access by FALCON-DARTTS users to the trade data stored in this subsystem occurs through one of two web applications: (1) ICE HSI and CBP users are granted access to all U.S. and foreign trade data via an internal DHS FALCON-DARTTS web application that resides within the DHS/ICE network, and (2) foreign

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

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

users are granted access to select trade datasets via a different web application that resides within a protected infrastructure space between the DHS Internet perimeter and the DHS/ICE network. Foreign users are able to access only the trade data related to their country and the related U.S. trade transactions unless access to other partner countries' data is authorized via information sharing agreements.

3. Technology and Methodology

FALCON-DARTTS uses COTS software to assist its users in identifying suspicious trade transactions by analyzing trade and financial data and identifying data that is statistically anomalous. In response to user-specified queries, the software application is designed to analyze structured and unstructured data using three tools: the drill-down technique,[97] link analysis, and charting and graphing tools that use proprietary statistical algorithms.[98] It also allows non-technical users with investigative experience to analyse large quantities of data and rapidly identify problem areas. The program makes it easier to apply their specific knowledge and expertise to complex sets of data.

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

FALCON-DARTTS can also identify links between individuals and/or entities based on commonalities, such as identification numbers, addresses, or other information. These commonalities in and of themselves are not suspicious, but in the context of additional information, they can assist investigators in identifying potentially criminal activity and lead to identification of witnesses, other suspects, or additional suspicious transactions.

FALCON-DARTTS uses trade data, financial data, and law enforcement data provided by other U.S. government agencies and foreign governments (hereafter referred to as "raw data").[99] ICE receives data from the sources listed below via CD-ROM, external storage devices, or electronic data transfers and loads the data into FALCON-DARTTS and the FALCON general data storage environment. The agencies that provide FALCON-DARTTS with trade data collect any PII

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

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

[99] 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.

directly from individuals or enterprises completing import-export electronic or paper forms.[100] Agencies that provide FALCON-DARTTS with financial data receive PII from individuals and institutions, such as banks, which are required to complete certain financial reporting forms.[101] PII in the raw data is necessary to link related transactions together. It is also necessary to identify persons or entities that should be investigated further.

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

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

Similarly, HSI investigators may access U.S. and foreign financial data from FALCON-DARTTS in FALCON-SA to conduct additional analysis and investigation using the tools and additional data available in FALCON-SA. These datasets are routinely ingested into FALCON-SA, and only FALCON-SA users who are also granted FALCON-DARTTS privileges will be authorized to access the financial data via the FALCON-SA interface.

4. Data Sources

All raw data analyzed by FALCON-DARTTS is provided by other U.S. agencies and foreign governments, and is divided into the following broad categories: U.S. trade data, foreign trade data, financial data, and law enforcement data. U.S. trade data is (1) import data in the form of an extract from ACS, which CBP collects from individuals and entities importing merchandise into the United States who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via ACS; (2) EEI submitted to AES; and (3) bill of lading data collected by

[100] 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.

[101] 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.

CBP via the AMS and provided to ICE through electronic data transfers for upload into FALCON-DARTTS.

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

ICE may receive U.S. financial data from FinCEN or federal, state, and local law enforcement agencies. Bank Secrecy Act (BSA) data is in the form of the following financial transaction reports: CMIRs (transportation of more than $10,000 into or out of the United States at one time); Currency Transaction Reports (deposits or withdrawals of more than $10,000 in currency into or from a domestic financial institution); Suspicious Activity Reports (information regarding suspicious financial transactions within depository institutions, money services businesses,[102] the securities and futures industry, and casinos and card clubs); Reports of Coins or Currency Received in a Non-Financial Trade or Business (transactions involving more than $10,000 received by such entities); and data provided in Reports of Foreign Bank and Financial Accounts (reports by U.S. persons who have financial interest in, or signature or other authority over, foreign financial accounts in excess of $10,000). Other financial data collected by other federal, state, and local law enforcement agencies is collected by such agencies in the course of an official investigation, through legal processes, and/or through legal settlements and has been provided to ICE to deter international money laundering and related unlawful activities.[103]

ICE receives law enforcement records from the Specially Designated Nationals (SDN) List and CBP's TECS system (subject records). In addition to listing individuals and companies owned or controlled by, or acting on behalf of, targeted countries, the SDN List includes information about foreign individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Their assets are blocked, and U.S. persons and entities are generally prohibited from dealing with them. FALCON-DARTTS analysis of the SDN List allows ICE HSI users to rapidly determine whether international trade and/or financial transactions with a specially designated individual or entity are being conducted, thus providing ICE HSI with the ability to take appropriate actions in a timely and more efficient manner.

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

[102] Under 31 U.S.C. § 5318, a money services business (MSB) is required by the BSA to complete and submit Suspicious Activity Reports to FinCEN. Entities qualifying as MSBs are defined under 31 C.F.R. § 1010.100(ff). They include money transmitters; issuers; redeemers and sellers of money orders and travelers' checks; and check cashers and currency exchangers. FinCEN administers the BSA, which requires financial depository institutions and other industries vulnerable to money laundering to take precautions against financial crime, including reporting financial transactions possibly indicative of money laundering. 31 U.S.C. §§ 5311-5330.

[103] For example, a court may direct a corporation to provide data to law enforcement agencies after determining that the corporation did not practice due diligence to deter money laundering and/or has facilitated criminal activities.

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

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

5. Efficacy

Through the use of FALCON-DARTTS, domestic HSI field offices and foreign attaché offices have the ability to initiate and enhance criminal cases related to trade-based money laundering and other financial crimes. Information derived from FALCON-DARTTS was essential in several criminal prosecutions and enforcement actions both domestically and abroad. For example, HSI Miami used information gathered through trade and financial queries in FALCON-DARTTS to assist in an investigation of a company involved in laundering of funds from illegal gold smuggling activities. The company was found to import scrap gold into the United States from Guatemala with declared amounts that were significantly undervalued. In January 2014, the company's owners were arrested in the Southern District of Florida for violations of 18 U.S.C. § 1956 (laundering of monetary instruments), 18 U.S.C. § 542 (entry of goods by means of false statements), and 18 U.S.C. § 545 (smuggling goods into the United States).

FALCON-DARTTS analytics were also used in support of an HSI Los Angeles investigation related to the unlawful importation of Chinese-made garments. The investigation revealed that the garments were deliberately misclassified in value during the import process and unlawfully exported to Mexico using a complex undervaluation scheme. The investigation also identified business employees who coordinated bulk currency deliveries derived from narcotics sales. In September 2014, HSI Los Angeles made arrests for money laundering and financial reporting requirements violations. In addition, HSI Los Angeles, in coordination with several other federal and state law enforcement agencies, executed multiple search warrants at residences and business locations centered in the Los Angeles Fashion District for money laundering, unlicensed money remitter, entry of goods by means of false statements, and smuggling of goods into and from the United States. During the operation, HSI Los Angeles seized over $90 million in bulk currency.

6. Laws and Regulations

ICE is authorized to collect the information analyzed by FALCON-DARTTS pursuant to the Trade Act of 2002 § 343, 19 U.S.C. § 2071 Note; 19 U.S.C. § 1484; and 31 U.S.C. § 5316. ICE HSI has the jurisdiction and authority to investigate violations involving the importation or exportation of merchandise into or out of the United States. Information analyzed by FALCON-DARTTS supports, among other things, HSI's investigations into smuggling violations under 18

U.S.C. §§ 541, 542, 545, and 554; money laundering investigations under 18 U.S.C. § 1956; and merchandise imported in non-compliance with 19 U.S.C. §§ 1481 and 1484. DHS is authorized to maintain documentation of these activities pursuant to 19 U.S.C. § 2071 Note (Cargo Information) and 44 U.S.C. § 3101 (Records Management by Agency Heads; General Duties). Information analyzed by FALCON-DARTTS may be subject to regulation under the Privacy Act of 1974,[104] the Trade Secrets Act,[105] and BSA.[106]

7. Privacy Impact and Privacy Protections

ICE does not use FALCON-DARTTS to make unevaluated decisions about individuals; FALCON-DARTTS is used solely as an analytical tool to identify anomalies. It is incumbent upon the HSI investigator to further investigate the reason for an anomaly. HSI investigators gather additional facts, verify the accuracy of the FALCON-DARTTS data, and use their judgment and experience to determine whether an anomaly is, in fact, suspicious and warrants further investigation for criminal violations. HSI investigators are required to obtain and verify the original source data from the agency that collected the information to prevent inaccurate information from propagating. All information obtained from FALCON-DARTTS is independently verified before it is acted upon or included in an HSI investigative or analytical report.

FALCON-DARTTS data is generally subject to access requests under the Privacy Act and FOIA and requests for amendment under the Privacy Act, unless a statutory exemption covering specific data applies. U.S. and foreign government agencies that collect information analyzed by FALCON-DARTTS are responsible for providing appropriate notice on the forms used to collect the information, or through other forms of public notice, such as SORNs.[107] FALCON-DARTTS will coordinate requests for access or to amend data with the original data owner. ICE published a PIA for FALCON-DARTTS on January 16, 2014, and republished the SORN that applies to FALCON-DARTTS on December 1, 2014.[108]

All raw data analyzed by FALCON-DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority. Therefore, FALCON-DARTTS relies on the systems and/or programs performing the original collection to provide accurate data. The majority of the raw data used by FALCON-DARTTS is accurate because the data was collected directly from the individual or entity to whom the data pertains. Due to the law enforcement

[104] 5 U.S.C. § 552a.

[105] 18 U.S.C. § 1905.

[106] 31 U.S.C. § 5311.

[107] The following SORNs are published in the Federal Register and describe the raw data ICE receives from U.S. agencies for use in FALCON-DARTTS: for FinCEN Information, Suspicious Activity Report System (Treasury/FinCEN .002) and BSA Reports System (Treasury/FinCEN .003) (updates for both of these SORNs were published at77 FR 60014 (Oct. 1, 2012), available at http://www.gpo.gov/fdsys/pkg/FR-2012-10-01/pdf/2012-24017.pdf), and for CBP Information, ACE/International Trade Data System (DHS/CBP-001) 71 FR 3109 (Jan. 19, 2006), available at http://www.gpo.gov/fdsys/pkg/FR-2006-01-19/html/E6-511.htm), ACS (Treasury/CS.278) (73 FR 77759 (Dec. 19, 2008), available at http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29801.htm), and TECS (DHS/CBP-011) (73 FR 77778 (Dec. 19, 2008), available at http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm).

[108] FALCON-DARTTS is covered by the SORN for the ICE Trade Transparency and Analysis Research (TTAR) system of records (79 FR 71112 (Dec. 1, 2014)).

context in which FALCON-DARTTS is used, however, there are often significant impediments to directly verifying the accuracy of information with the individual to whom the specific information pertains.[109] In the event that errors in raw data are discovered by FALCON-DARTTS users, the FALCON-DARTTS system owner will notify the originating agency. All raw data analyzed by FALCON-DARTTS is updated at least monthly for all sources, or as frequently as the source system can provide updates or corrected information.

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

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

As FALCON-DARTTS is a component system of the larger ICE HSI FALCON environment, FALCON-DARTTS uses the access controls, user auditing, and accountability functions described in the FALCON-SA PIA. For example, user access controls allow data access to be restricted at the record level, meaning that only datasets authorized for a user-specific profile are visible and accessible by that user. Audit capabilities log user activities in a user activity report, which is used to identity users who are using the system improperly.[110]

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

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

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

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

In 2009, NARA approved a record retention period for the information maintained in the legacy DARTTS system. As noted in the 2014 FALCON-DARTTS PIA, ICE intends to request NARA approval to retire the legacy DARTTS records retention schedule and incorporate the retention periods for data accessible by FALCON-DARTTS into the forthcoming records schedule for the FALCON environment. The datasets used by FALCON-DARTTS will be retained for ten years. Some of the data used by FALCON-DARTTS is already maintained in the FALCON general data storage environment and subject to a proposed retention period; however, FALCON-DARTTS will only access these existing datasets for ten years. Several new datasets were added to the FALCON general storage environment with the launch of FALCON-DARTTS, and the retention and access period for those datasets is proposed to be ten years as well.

D. FALCON-Roadrunner

1. 2014 Program Update

In November 2014, ICE launched FALCON-Roadrunner, a system that was described in the 2013 DHS Data Mining Report as under development.[111] FALCON-Roadrunner enables ICE HSI investigators and analysts to conduct trend analysis and generate investigative leads that are used to identify illicit procurement networks, terrorists groups, and hostile nations attempting to illegally obtain U.S. military products; sensitive dual-use technology; weapons of mass destruction; or chemical, biological, radiological, and nuclear materials. The system also provides HSI users the ability to perform research and generate leads for investigations of export violations within the jurisdiction of HSI. FALCON-Roadrunner analyzes trade, financial, law enforcement, and screening data across large, disparate datasets to identify statistically anomalous trade transactions that may warrant investigations of export violations. FALCON-Roadrunner is a module within ICE's existing FALCON environment, which is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other federal, state, local, and foreign government and private sector sources, with appropriate user access restrictions and robust user auditing controls.[112]

ICE published the FALCON-Roadrunner PIA on November 12, 2014.[113] On December 1, 2014, ICE republished the Trade Transparency Analysis and Research (TTAR) SORN to expand its coverage to FALCON-Roadrunner.[114] Lastly, ICE plans to update the FALCON-SA PIA Appendix to capture the immigration, law enforcement, and publicly available FALCON-

[111] 2013 Data Mining Report at p. 9.

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

[113] *See* DHS/ICE/PIA-040 FALCON-Roadrunner, November 12, 2014, http://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-falconroadrunner-november2014.pdf.

[114] *See* DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, 79 FR 71112 (Dec. 1, 2014), http://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm.

Roadrunner data that is being stored in the FALCON environment and made accessible to additional users through FALCON-SA's user interface.

2. Program Description

One of ICE's highest enforcement priorities is to prevent illicit procurement networks, terrorist groups, and hostile nations from illegally obtaining U.S. military products; sensitive dual-use technology;[115] weapons of mass destruction; or chemical, biological, radiological, and nuclear materials. The HSI Counter-Proliferation Investigations (CPI) Program oversees a broad range of investigative activities related to such violations of law. The CPI Program enforces U.S. laws governing the export of military items, controlled dual-use goods, firearms, and ammunition, as well as exports to sanctioned or embargoed countries.

FALCON-Roadrunner provides two services in support of the CPI Program:

- *Investigative Lead Generation*: FALCON-Roadrunner allows CPI investigators and analysts to generate leads for, and otherwise support, investigations of export violations within the jurisdiction of HSI. By using FALCON-Roadrunner to analyze trade data, CPI investigators and analysts are able to identify anomalous transactions and activities that may be indicative of export violations and warrant investigation. Experienced HSI investigators independently confirm and further investigate these anomalies.

- *Statistical/Trend Analysis*: FALCON-Roadrunner provides export enforcement-related statistical reporting capabilities, derived from trade data that investigators access. Statistical analytics and trend analysis is provided to the Export Enforcement Coordination Center, which is the primary forum within the Federal Government for executive departments and agencies to coordinate and enhance their export control enforcement activities.

FALCON-Roadrunner is owned and operated by the CPI Program and made accessible to approved users via the ICE enterprise network. Only CPI investigators, analysts, and contractors are authorized to use the system. The results of FALCON-Roadrunner analyses are forwarded to ICE HSI field offices as part of an investigative referral package to initiate or support a criminal investigation. FALCON-Roadrunner allows users to perform research and analyses that are not possible in any other ICE system because of the unique capabilities of the technology it uses, the data available for analysis, and the level of detail at which the data can be analyzed. As part of the CPI investigative process, FALCON-Roadrunner users are seeking to understand and assess the relationships between importers, exporters, manufacturers, commodity end-users, shippers, denied parties, licensing, export controls, and financing for each and every trade transaction to determine which are suspicious and warrant further investigation. If performed manually, this process would involve hours or even days of analysis of voluminous data and may not reveal potential violations due to the sheer volume and complexity of the data.

[115] Goods and technologies are considered to be dual-use when they can be used for both civil and military purposes, such as special materials, sensors and lasers, and high-end electronics.

3. Technology and Methodology

FALCON-Roadrunner allows users[116] to run complex search queries that assess massive volumes of trade transactions. These queries provide investigative leads and interdiction targets by identifying anomalies and non-obvious patterns and relationships within and across multiple large-scale trade, law enforcement, and other datasets. For example, FALCON-Roadrunner gives users the tools to work with multiple disparate datasets containing data elements of interest, and perform data filters or queries based on CPI-focused criteria thereby reducing millions of records to a more manageable quantity that they can then further investigate. This process and use of technology provides for a more robust method to identify non-obvious relationships within very large quantities of data.

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

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

FALCON-Roadrunner's system architecture has three basic levels:

(1) A foundational or data storage layer managed with COTS software.

(2) An analytical layer with two COTS applications that permit data to be displayed in a variety of ways, using a variety of filters. Data results from the use of one filter can be verified by using alternate filters.

[116] In respect to the discussion of FALCON-Roadrunner, the term "user," shall be understood as meaning 'ICE HSI Counter-Proliferation Investigations (CPI) Unit investigators and analysts.'

(3) A “Widget Manager,” which is a government off-the-shelf product, to allow users to access the tools from a single platform.

Pattern and anomaly detection is at the discretion of the user. A rule or data filter is applied to the data. The rule is created based on the investigator or analyst’s knowledge of data in a particular data set, and the factors that could constitute an anomaly. For example, if the investigator or analyst wishes to determine potential smugglers of sensitive material, the investigator/analyst will need to know which data points the system should focus on in order to identify what he/she feels is an anomaly. There is no automated method to identify anomalies – all results have to be visually inspected to determine acceptance as an anomaly. Queries can be saved, however, for repetitive use and use by others with permission to access the system.

Since FALCON-Roadrunner is an analytical tool over the larger FALCON environment, the datasets FALCON-Roadrunner analyzes are stored in the FALCON general data storage environment and are available to FALCON-Roadrunner users for additional analysis and investigation using the tools and additional data that is available in FALCON-SA. Some of the data available to FALCON-Roadrunner users is also made available to FALCON-SA users, while other data will only be available in FALCON-SA if the user also has Roadrunner privileges. FALCON-SA enforces these access restrictions by requiring users with FALCON-Roadrunner privileges to designate their investigations within the system as CPI investigations; otherwise, the datasets specific to FALCON-Roadrunner will not be available for use and analysis in FALCON-SA. As discussed in Section 4, FALCON-Roadrunner adds new immigration, law enforcement, and publicly available data to the FALCON general data storage environment. ICE is updating the FALCON-SA PIA Appendix to reflect the new data is available via FALCON-SA as a result of the FALCON-Roadrunner system coming online.

4. Data Sources

FALCON-Roadrunner uses various categories of data collected by other agencies, foreign governments, and commercial sources (hereafter referred to as “raw data”). With the exception of ICE TECS records and visa security information, all raw data used for FALCON-Roadrunner is provided by other U.S. government agencies, foreign governments, and commercial sources. The raw data sources are divided into the following broad categories: U.S. trade data, foreign trade data, screening lists, financial data, law enforcement data, and commercial data.

U.S. trade data is (1) import data in the form of extracts from ACS, which CBP collects from individuals and entities importing merchandise into the United States that complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via the Automated Commercial Environment and (2) export data in the form of EEI[117] that CBP collects from individuals and entities exporting merchandise from the United States.

[117] EEI is the export data as filed in AES, *see* http://export.gov/logistics/aes/index.asp. This data is the electronic equivalent of the export data formerly collected as Shipper’s Export Declaration information. This information is now mandated to be filed through the AES or Automated Export System *Direct, see* http://aesdirect.census.gov. AES is operated jointly by the U.S. Census Bureau and CBP. *See* DHS/CBP/PIA-020 Export Information System (EIS), available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-eis-01312014.pdf.

Foreign import and export data analyzed by FALCON-Roadrunner is provided to ICE by foreign law enforcement and customs officials pursuant to CMAAs or other similar information sharing agreements. Certain countries provide trade data that has been stripped of PII. Other countries provide complete trade data, including the names of businesses and individuals and other identifying information that may be contained in the trade records.

Screening list data is produced by government entities and contains information on individuals and entities that are prohibited from engaging in certain trade transactions. These screening lists include: the publicly available European Union Denied Party Screening Lists[118] and the publicly available consolidated U.S. export screening lists of the U.S. Department of Commerce, State, and Treasury.[119] The consolidated U.S. export lists serve as an aid to industry in conducting electronic screens of potential parties to regulated transaction. Additional detail about the contents of this screening list is included in Section 2.2 of the FALCON-Roadrunner PIA.

ICE receives financial data from other federal, state, and local law enforcement agencies that collected the data in the course of an official investigation, through legal processes, or legal settlements, or both, and has been provided to ICE to deter international money laundering and related unlawful activities.[120]

ICE receives law enforcement records from CBP's TECS system (subject and investigative records) and visa security data from DoS. TECS subject records include Person Subject, Vehicle Subject, Vessel Subject, Aircraft Subject, Thing Subject, Business Subject, and Organization Subject records. TECS investigative records concern current or previous law enforcement investigations into violations of U.S. customs and immigration laws, as well as other laws and regulations within ICE's jurisdiction, including investigations led by other domestic or foreign agencies when ICE is providing support and assistance.[121]

Visa security data is collected by DoS directly from visa applicants as part of the visa application process. The data is then provided to DHS for security review, and is stored in ICE's VSPTS-Net system. It is ingested from VSPTS-Net into the FALCON environment via a system to system connection.[122]

[118] In order to facilitate the application of financial sanctions, the Banking Federation of the European Union, the European Savings Banks Group, the European Association of Co-operative Banks, the European Association of Public Banks (EU Credit Sector Federations), and the European Commission created an EU consolidated list of persons, groups, and entities subject to Common Foreign and Security Policy-related financial sanctions. The consolidated list database was developed to assist the members of the EU Credit Sector Federations in their compliance with financial sanctions. *See* http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm.

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

[120] For example, a court may direct a corporation to provide data to law enforcement agencies after determining that the corporation did not practice due diligence to deter money laundering and/or has facilitated criminal activities.

[121] *See* DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf; DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf. *See also* DHS/CBP-011 U.S. Customs and Border Protection TECS SORN, 73 FR 77778 (Dec. 19, 2008), available at http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

[122] *See* DHS/ICE/PIA-011(a) Visa Security Program Tracking System-Network version 2.0 available at http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia-

Lastly, FALCON-Roadrunner ingests commercially available counter-proliferation data to screen commodity end-users, individuals, and other parties involved in a transaction against both denied parties (e.g., individuals and entities that have been denied export privileges) and profiles of entities determined by an outside independent group to have some level of risk for illicit proliferation of nuclear technology, commodities, or weapons delivery systems. The system also contains commercially available business insights about companies based on the sectors in which they participate through the sale of products and services, the companies' interconnecting supply chain relationships, and the companies' geographic revenue exposure. This information is compiled from publicly available press releases, investor presentations, corporate actions, and Internet queries.

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

5. Efficacy

Because FALCON-Roadrunner became operational near the close of the reporting period, it is premature to describe the system's efficacy in the 2014 DHS Data Mining Report. A detailed discussion of the efficacy of FALCON-Roadrunner will be included in future DHS Data Mining Reports.

6. Laws and Regulations

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

7. Privacy Impact and Privacy Protections

Any law enforcement investigation that is initiated as a result of a FALCON-Roadrunner analysis will, from that point forward, be carried out like any other criminal investigation. ICE will follow normal investigatory protocols and the same civil liberties and constitutional restrictions, such as the Fourth Amendment's probable cause requirements, will apply. CPI Unit investigators and analysts are prohibited from taking a law enforcement action against an individual or entity based on data and analysis from FALCON-Roadrunner alone. FALCON-Roadrunner is a system designed to help investigators generate leads for new or existing investigations. CPI investigators and analysts will fully investigate leads generated by FALCON-Roadrunner analyses before taking action against an individual or entity. To ensure

ice_vspts%20net%202%200_20130117.pdf and DHS/ICE-012 Visa Security Program Records SORN, 74 FR 50228 (Sept. 30, 2009), available at http://www.gpo.gov/fdsys/pkg/FR-2009-09-30/html/E9-23522.htm.

they have the best evidence available to support any case they are building, the investigators obtain the needed information from the original data sources and further investigate the reason for the anomaly. If the anomaly can be legitimately explained, there is no need to further investigate for criminal violations. Any and all information obtained from FALCON-Roadrunner will be independently verified before it is acted upon or included in an ICE investigative or analytical report.

FALCON-Roadrunner data is generally subject to access requests under the Privacy Act and FOIA and requests for amendment under the Privacy Act, unless a statutory exemption covering specific data applies. U.S. and foreign government agencies that collect information analyzed by FALCON-Roadrunner are responsible for providing appropriate notice on the forms used to collect the information, or through other forms of public notice, such as SORNs.[123] FALCON-Roadrunner will coordinate requests for access or to amend data with the original data owner. ICE published a PIA for FALCON-Roadrunner on November 12, 2014, and republished the SORN that applies to FALCON-Roadrunner on December 1, 2014.[124]

With the exception of ICE TECS records and visa security information, all information in FALCON-Roadrunner is obtained from other governmental organizations that collect the data under specific legislative authority or from commercial vendors. The original data collector is responsible for maintaining and checking the accuracy of its own data and has various means to do so. The majority of the data loaded into FALCON-Roadrunner is highly accurate because the data was collected by third parties directly from the individual or entity to which the data pertains. In other instances, however, the data about individuals or entities is provided to the governmental organization by a third party. Commercial vendors are considered to have a financial incentive to provide high-quality and accurate data to their customers. The system owner and users are aware that they cannot independently verify the accuracy of the bulk data the system receives. FALCON-Roadrunner is updated when corrected data is received from the collecting governmental organizations and commercial vendors. In the event that errors are discovered, the FALCON-Roadrunner system owner will notify the originator of the data. The system owner will remove datasets that are found over time to have poor data quality from FALCON-Roadrunner.

Access to FALCON-Roadrunner is limited to HSI investigators and analysts who conduct official CPI activities. Access privileges are only granted by the FALCON system administrator with the explicit written permission of the FALCON-Roadrunner Program Manager. FALCON-Roadrunner privileges are evaluated on a case-by-case basis.

The FALCON environment, of which FALCON-Roadrunner is a component, was granted an ongoing Security Authorization on November 6, 2013. Any violations of system security or

[123] The following SORNs are published in the Federal Register and describe the raw data ICE receives from U.S. agencies for use in FALCON-Roadrunner: DHS/CBP-015 Automated Commercial System (ACS) SORN, 73 FR 77759 (Dec. 19, 2008); DHS/CBP-001 Automated Commercial Environment/International Trade Data System (ACE/ITDS) SORN, 71 FR 3109 (Jan. 19. 2006); DHS/CBP-011 TECS SORN, 73 FR 77778 (Dec. 19, 2008); DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, 79 FR 71112 (Dec. 1, 2014); DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN, 75 FR 9233 (Mar. 1, 2010); and DHS/ICE-012 Visa Security Program Records SORN, 74 FR 50228 (Sept. 30, 2009).

[124] FALCON-Roadrunner is covered by the SORN for the ICE Trade Transparency Analysis and Research (TTAR) system of records (79 FR 71112) (Dec. 1, 2014)).

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. Since FALCON-Roadrunner is part of the larger FALCON environment, the system uses the same access controls, user auditing, and accountability as those described in the FALCON-SA PIA. For more information on these, please see the FALCON-SA PIA.[125]

As noted in the 2014 FALCON-Roadrunner PIA, ICE intends to incorporate the retention periods for data accessible by FALCON-Roadrunner into the forthcoming records schedule for the FALCON environment. The data used by FALCON-Roadrunner will be accessed for ten years. Some of the data used by FALCON-Roadrunner is already maintained in the FALCON general data storage environment and subject to a proposed retention period; however, FALCON-Roadrunner will only access these existing datasets for ten years. Several new datasets were added to the FALCON general storage environment with the launch of FALCON-Roadrunner, and the retention and access period for those datasets is proposed to be ten years as well.

E. DHS Data Framework

1. 2014 Program Update

From November 2013 to August 2014, DHS deployed a pilot/prototype to test different capabilities needed to implement the DHS Data Framework.[126] After the successful completion of the pilot/prototype phase, DHS now intends to mature the Framework by entering into the next phase—limited production capability.[127]

The Department used three data sets in the pilot/prototype phase: CBP's ESTA, ICE's SEVIS, and TSA's Alien Flight Student Program (AFSP). The data sets were copied from the relevant component IT system, transferred into the Neptune platform and tagged, and then the tagged data elements were pushed to the Common Entity Index (CEI) and Cerberus platforms. The pilot/prototype phase successfully demonstrated important foundational elements of the Framework, including, but not limited to those capabilities described below.

[125] *See* DHS/ICE/PIA-032 – FALCON Search & Analysis System (FALCON-SA), February 1, 2012, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_falconsa.pdf.

[126] The Neptune Pilot PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-neptune-09252013.pdf. The Common Entity Index (CEI) Prototype PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-cei-pilot-_09262013.pdf. The Cerberus Pilot PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-cerberus-nov2013.pdf. The DHS Data Framework PIA is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

[127] The updated Data Framework PIA for limited production capability is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-pia-046-a-dhs-data-framework-08292014.pdf. The updated Neptune PIA for limited production capability is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-046-1-a-neptune-08292014.pdf. The updated Cerberus PIA for limited production capability is available at http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-DHS-ALL-PIA-046-3-a-Cerberus-08292014.pdf.

- *Data Management and Transfer*: The pilot/prototype phase demonstrated that Neptune could ingest the data from the three datasets, apply access control tags and relevant metadata, and transfer the tagged data to the CEI and Cerberus. The data tags identified the type of data involved, when the data originated, when it was ingested as authoritative mission data, and whether the data elements are designated as core, extended, or encounter.[128]
- *User Authentication and Attributed-Based Access*: The pilot/prototype phase demonstrated users could be authenticated with appropriate certificates and that their attributes were properly set with predetermined functions and purposes. Upon login, a user's attributes were retrieved from an attribute authority. Where a user had more than one function and purpose (i.e., the user needed access to data while acting in different capacities), the user was able to select the appropriate functions and purposes for accessing data. Once a user was positively authenticated, the user would have access to the Cerberus system and could request data.
- *Policy-Based Access Control*: The pilot/prototype phase demonstrated that DHS could apply policy-based access controls to determine the type of basic search tools the user could use and what data the user could access. Given a particular user's attributes, an Access Control Server asked what function and purpose the user performs to then determine what privileges the user had. The user's function controlled the basic search tools (i.e., the type of query that could be performed) that the user could use. The user's purpose determined which data sets and which type of data (i.e., core, extended, or encounter) the user could access. The Department tested a variety of purpose and function combinations to test whether the Access Control Server gave the user access to the correct tools and data. In each instance, the demonstrations showed that the policy-based controls were appropriately applied and that users only had access to the search tools, data sets, and types of data that they were permitted to access under DHS policy.
- *Audit Logging*: The pilot/prototype phase also demonstrated that DHS could log the application of policy-based controls as it was occurring. The policy decision log showed the policy enforcement when a user requested access and evaluating the policy rules to determine the user's privileges to data or tools. The audit log reader also captured the queries a user made and statistics regarding query results, aiding in audit and oversight, including verification of compliant data usage.

Because the Framework controls are still maturing, access to the integrated data and tools will remain limited through the policy-based controls for user functions and purposes defined in the pilot/prototype phase. The data sets and basic search tools will also remain the same. Specifically, the search tools used during limited production capability are the three basic search functions deployed in the pilot/prototype phase: person search, characteristic search, and trend search. Similarly, limited production capability will involve a pre-approved number of users from selected components, no new information sharing roles from those previously established, and limited production capability respects current access controls embedded in operational systems.

[128] Additional information about these terms can be found in the DHS Data Framework PIA.

Limited production capability will include an initial bulk data ingest of the source systems (i.e., a ‘snapshot’ in time) into Neptune, followed by increased instances of data refreshes as the limited production capability progresses. The goal was to have regular data refreshes of the source systems by the end of 2014. Cerberus users will be trained to understand the risk associated with data latency and to verify information at the source system. Until continuous data updates can be accomplished, no operational use of the data will occur without a human review and verification of the information within the source system. To facilitate this human review, data is tagged with the source system and contact information.

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

2. Program Description

DHS developed the DHS Data Framework, a scalable information technology program with built-in capabilities to support advanced data architecture and governance processes. The Framework is DHS’s “big data” solution to build in privacy protections while enabling more controlled, effective, and efficient use of existing homeland security-related information across the DHS enterprise and with other U.S. Government partners, as appropriate. This program alleviates mission limitations associated with stove-piped IT systems that are currently deployed across multiple operational components in DHS. It also enables more controlled, effective, and efficient use and sharing of available homeland security-related information across the DHS enterprise and, as appropriate, the U.S. Government, while protecting privacy. Currently, the Framework includes the Neptune and Cerberus systems, and the CEI.

DHS changed the way it structures its information architecture and data governance to further consolidate information in a manner that protects individuals’ privacy, civil rights, and civil liberties. Existing information maintained by the Department is subject to privacy, civil rights and civil liberties, and other legal and policy protections, and it is collected under different authorities and for various purposes. The existing architecture of DHS databases, however, is not conducive to effective implementation of the “One DHS” policy, which was implemented to afford DHS personnel timely access to relevant and necessary homeland-security information they need to successfully perform their duties and protect the Homeland.[129] Currently, this access is cumbersome, time-intensive, and requires personnel to log on and query separate databases in order to determine what information DHS systems contain about a particular individual. The goal of the DHS Data Framework is to provide a user the ability to search an amalgamation of data extracted from multiple DHS systems for a specific purpose and to view

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

the information in a clear and accessible format. The DHS Data Framework enables efficient and cost-effective searches across DHS databases in both classified and unclassified domains.

The DHS Data Framework defines four elements for controlling data:

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

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

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

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

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

3. Technology and Methodology

Initially, the data tags, context, and dynamic access was tested to enable greater information sharing and comparison in support of operations and to build in greater privacy protections. The DHS Data Framework incorporates a User Attribute Hub, which maintains a listing of a system user's attributes for determining access control (e.g., component in which the individual works, location, job series). This attribute hub is developed through a different effort by the DHS Office of the Chief Information Officer. The following capabilities tested the other three elements of the Framework using data from ESTA,[130] SEVIS,[131] and AFSP.[132]

- *Neptune Pilot:* The Neptune Pilot, residing in the SBU/ FOUO domain, ingests and tags data in a data repository known as "Neptune." This pilot tests the second element of the DHS Data Framework (data tags). Data in the Neptune Pilot is shared with the CEI Prototype and the Cerberus Pilot, but will ***not*** be accessible for other purposes.

- *CEI Prototype:* The CEI Prototype, also residing on the SBU/FOUO domain, receives a subset of the tagged data from the Neptune Pilot and correlates data from across component datasets. The CEI Prototype tests the utility of the Neptune-tagged data—specifically, the ability to ensure that only users with certain attributes are able to access data based on defined purposes using the dynamic access control process. This prototype uses data tags to test the third and fourth elements of the DHS Data Framework (context and dynamic access control, respectively).

[130] *See* DHS/CBP/PIA-007(c), ESTA Update, June 5, 2013; DHS/CBP/PIA-007(b) ESTA - Internet Protocol Address and System of Records Notice Update, July 18, 2012; DHS/CBP/PIA-007(a) ESTA Fee and Information Sharing Update, July 18, 2011; DHS/CBP/PIA-007 ESTA June 2, 2008, available at www.dhs.gov/privacy.

[131] *See* DHS/ICE/PIA-001(a) SEVIS Update National Counter Terrorism Center, June 23, 2011; DHS/ICE/PIA-001 – SEVIS, February 5, 2005, available at www.dhs.gov/privacy.

[132] DHS/TSA/PIA-026 AFSP, July 28, 2014, available at http://www.dhs.gov/sites/default/files/publications/privacy_pia_tsa%20alien%20flight%20student%20program_july%202014.pdf.

- *Cerberus Pilot:* The Cerberus Pilot, residing in the Top Secret/Sensitive Compartmented Information (TS/SCI) domain, receives all of the tagged data from the Neptune Pilot in a separate data repository known as Cerberus. The Cerberus Pilot tests the ability to ensure that only users with certain attributes are able to access data based on defined purposes using the dynamic access control process. This pilot leverages the data tags to test the context and dynamic access control elements of the DHS Data Framework. The Cerberus Pilot also tests the ability to perform simple and complex searches across different component datasets using different analytical tools.

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

4. Data Sources

The Department used three datasets in the pilot/prototype phase: ESTA,[133] SEVIS,[134] and AFSP.[135] The datasets were copied from the relevant component IT system, transferred into the Neptune platform and tagged, and then the tagged data elements were pushed to the CEI and Cerberus platforms.

5. Efficacy

Based on the Framework's success to date, the Department is moving from the pilot/prototype phase to a limited production capability for both the Neptune and Cerberus systems. During limited production capability, DHS will test the ability to refresh data from the original DHS IT system to the Framework. The limited production capability shares many of the pilot/prototype phase conditions, except that limited production capability provides for limited evaluation in the operational environment. For example, the data elements the source systems transfers to Neptune for ingestion are the same as was in the Neptune Pilot. DHS will provide additional information in future Data Mining Reports on the efficacy of the Framework.

6. Laws and Regulations

Section 101 of the Homeland Security Act of 2002, Pub. Law No. 107-296 (Nov. 25, 2002), as amended, establishes DHS as an executive department of the United States. The mission of the Department is, among other things, to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, minimize the damage and assist in the recovery from terrorist attacks that do occur within the United States, support the missions of its

[133] *See* DHS/CBP/PIA-007(c), ESTA Update, June 5, 2013; DHS/CBP/PIA-007(b) ESTA - Internet Protocol Address and System of Records Notice Update, July 18, 2012; DHS/CBP/PIA-007(a) ESTA Fee and Information Sharing Update, July 18, 2011; DHS/CBP/PIA-007 ESTA June 2, 2008, available at www.dhs.gov/privacy.

[134] *See* DHS/ICE/PIA-001(a) SEVIS Update National Counter Terrorism Center, June 23, 2011; DHS/ICE/PIA-001 – SEVIS, February 5, 2005, available at www.dhs.gov/privacy.

[135] DHS/TSA/PIA-026 AFSP, July 28, 2014, available at http://www.dhs.gov/sites/default/files/publications/privacy_pia_tsa%20alien%20flight%20student%20program_july%202014.pdf.

legacy components, monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking. At the same time, the Department has the primary responsibility to ensure that the privacy, civil rights, and civil liberties of individuals are not diminished by efforts, activities, and programs aimed at securing the homeland.

DHS is changing the way it structures its information architecture and data governance to further consolidate information in a manner that protects individuals' privacy, civil rights, and civil liberties. The existing architecture of DHS databases, however, is not conducive to effective implementation of the "One DHS" policy.[136] Existing information is subject to privacy, civil rights and civil liberties, and other legal and policy protections, and it is collected under different authorities and for various purposes. Since 2007, DHS has operated under the "One DHS" policy, which was implemented to afford DHS personnel timely access to relevant and necessary homeland-security information they need to perform their duties successfully. Under this policy, DHS personnel requesting information maintained within another departmental component may access such information when the requestor (1) has an authorized purpose, mission, and need-to-know before accessing the information in performance of his or her duties; (2) possesses the requisite background or security clearance; and (3) assures adequate safeguarding and protection of the information. Currently, this access is cumbersome, time-intensive, and requires personnel to log on and query separate databases in order to determine what information DHS systems contain about a particular individual.

At present, the DHS Data Framework includes data from SEVIS,[137] ESTA,[138] AFSP.[139] The authorities and policies for each of these data sets are also applied in the DHS Data Framework. For more information on the specific authorities and policies associated with each data set, please see the relevant privacy impact assessments.[140]

[136] *DHS Policy for Internal Information Exchange and Sharing*, February 1, 2007.

[137] *See* DHS/ICE/PIA-001(a) Student and Exchange Visitor System (SEVIS) Update national Counter Terrorism Center, June 23, 2011; DHS/ICE/PIA-001 – Student and Exchange Visitor Information System (SEVIS), February 5, 2005, available at www.dhs.gov/privacy.

[138] *See* DHS/CBP/PIA-007(c) - Electronic System for Travel Authorization (ESTA) Update, June 5, 2013; DHS/CBP/PIA-007(b) Electronic System for Travel Authorization (ESTA) - Internet Protocol Address and System of Records Notice Update, July 18, 2012; DHS/CBP/PIA-007(a) Electronic System for Travel Authorization (ESTA) Fee and Information Sharing Update, July 18, 2011; DHS/CBP/PIA-007 Electronic System for Travel Authorization, June 2, 2008, available at www.dhs.gov/privacy.

[139] DHS/TSA/PIA-026 Alien Flight Student Program, July 28, 2014, available at http://www.dhs.gov/sites/default/files/publications/privacy_pia_tsa%20alien%20flight%20student%20program_july%202014.pdf.

[140] *See* DHS/ICE/PIA-001(a) Student and Exchange Visitor System (SEVIS) Update national Counter Terrorism Center, June 23, 2011; DHS/ICE/PIA-001 – Student and Exchange Visitor Information System (SEVIS), February 5, 2005, available at www.dhs.gov/privacy. *See* DHS/CBP/PIA-007(c) - Electronic System for Travel Authorization (ESTA) Update, June 5, 2013; DHS/CBP/PIA-007(b) Electronic System for Travel Authorization (ESTA) - Internet Protocol Address and System of Records Notice Update, July 18, 2012; DHS/CBP/PIA-007(a) Electronic System for Travel Authorization (ESTA) Fee and Information Sharing Update, July 18, 2011; DHS/CBP/PIA-007 Electronic System for Travel Authorization, June 2, 2008, available at www.dhs.gov/privacy. *See* DHS/TSA/PIA-026 Alien Flight Student Program, July 28, 2014, available at http://www.dhs.gov/sites/default/files/publications/privacy_pia_tsa%20alien%20flight%20student%20program_july%202014.pdf.

7. Privacy Impact and Privacy Protections

Robust privacy protections are the bedrock of the DHS Data Framework. Accordingly, DHS performed in-depth privacy impact assessments of the DHS Data Framework and its underlying components. Specifically, DHS has published privacy impact assessments for the DHS Data Framework itself,[141] Cerberus,[142] Neptune,[143] and CEI.[144] The privacy protections for the DHS Data Framework are numerous and multifaceted and are described in detail in these privacy impact assessments. DHS has updated these privacy impact assessments at each stage of the DHS Data Framework's maturation. Because the privacy impacts will continue to be assessed and additional privacy protections implemented as the program progresses, DHS will continue to update its privacy impact assessments as the program matures. For the most recent information on the DHS Data Framework's privacy impacts and protections, please see the relevant privacy impact assessments.[145]

IV. CONCLUSION

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

[141] *See* DHS/ALL/PIA-046 DHS Data Framework. Multiple iterations are available at www.dhs.gov/privacy.
[142] *See* DHS/ALL/PIA-046-3 Cerberus. Multiple iterations are available at www.dhs.gov/privacy.
[143] *See* DHS/ALL/PIA-046-1 Neptune. Multiple iterations are available at www.dhs.gov/privacy.
[144] *See* DHS/ALL/PIA-046-2 Common Entity Index. Multiple iterations are available at www.dhs.gov/privacy.
[145] *See* DHS/ALL/PIA-046 DHS Data Framework. Multiple iterations are available at www.dhs.gov/privacy. *See* DHS/ALL/PIA-046-3 Cerberus. Multiple iterations are available at www.dhs.gov/privacy. *See* DHS/ALL/PIA-046-1 Neptune. Multiple iterations are available at www.dhs.gov/privacy. *See* DHS/ALL/PIA-046-2 Common Entity Index. Multiple iterations are available at www.dhs.gov/privacy.

V. APPENDIX

Acronym List	
ABTC2	Ag/Bio-terrorism Rule Set
ACAS	Air Cargo Advance Screening
ACE	Automated Commercial Environment
ACS	Automated Commercial System
ADIS	Arrival and Departure Information System
ADIT	Alien Documentation and Identification Telecommunication
AES	Automated Export System
AFI	Analytical Framework for Intelligence
AFSP	Alien Flight Student Program
AMS	Automated Manifest System
APIS	Advance Passenger Information System
ATO	Authorization to Operate
ATS	Automated Targeting System
ATS-N	Automated Targeting System—Inbound Module
ATS-L	Automated Targeting System—Land Module
ATS-TF	Automated Targeting System—Targeting Framework
ATS-UPAX	Automated Targeting System—Unified Passenger Module
BCI	Border Crossing Information
BSA	Bank Secrecy Act
CBP	U.S. Customs and Border Protection
CCD	Consolidated Consular Database
CDC	Cross Domain Capabilities
CEI	Common Entity Index
CMAA	Customs Mutual Assistance Agreement
CMIR	The Report of International Transportation of Currency or Monetary Instruments Form
COP	Common Operating Picture
COTP	Captains of the Port
CTAC	Commercial Targeting and Analysis Center
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	U.S. Department of Homeland Security
DMV	Department of Motor Vehicles
DNBL	Do Not Board List
DOJ	U.S. Department of Justice
DoS	U.S. Department of State
EBSVERA	Enhanced Border Security and Visa Entry Reform Act of 2002
EEI	Electronic Export Information
ENFORCE	ICE Enforcement Case Management System / Enforcement Integrated

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

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