Department of Homeland Security

Privacy Office

2015 Data Mining Report to Congress
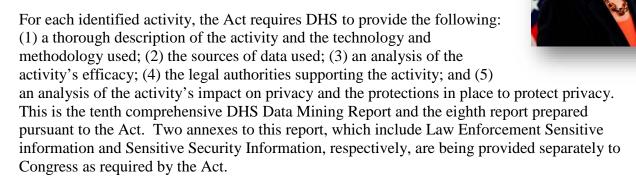
February 2016
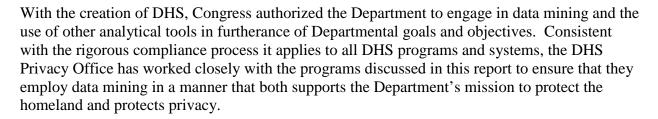
Homeland
Security

FOREWORD

February 2016

I am pleased to present the Department of Homeland Security's (DHS) 2015 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 tenth comprehensive DHS Data Mining Report and the eighth 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 Paul D. Ryan
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 (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 2014 DHS Data Mining Report,[2] the DHS Privacy Office discussed the following Departmental programs that engage in data mining, as defined by the 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 FALCON 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, 2015, through December 31, 2015, provides updates on modifications, additions, and other developments that have occurred during the reporting year. Additional information on DARTTS and 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. These programs contain Law Enforcement Sensitive Information and Sensitive Security Information, respectively.

The Homeland Security Act of 2002 expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[3] DHS exercises this authority with respect to 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 (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] 2014 DHS Data Mining Report available at:
http://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf
[3] 6 U.S.C. § 121(d)(13).
[4] 5 U.S.C. § 552a.
[5] 44 U.S.C. § 3501 note

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

The DHS Privacy Office implements the Chief Privacy Officer's authorities through privacy compliance policies and procedures, which are based on a set of eight Fair Information Practice Principles (FIPPs) rooted in the tenets of the Privacy Act. The FIPPs serve as DHS's core privacy framework. 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* (December 29, 2008)[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 DHS activities that involve data mining.

As described more fully below, the DHS Privacy Office's compliance process requires systems and programs collecting, ingesting, maintaining, and using Personally Identifiable Information (PII) and other information relating to individuals to complete, if required by law, federally-mandated privacy documentation. This documentation consists of a Privacy Impact Assessment (PIA), required by the E-Government Act,[9] and a System of Records Notice (SORN), 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, no decisions about individuals are made based solely on data mining results. In all cases, DHS employees analyze the results of data mining, and then apply their own judgment and expertise 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] 44 U.S.C. § 3501 note

[10] 5 U.S.C. § 552a(e)(4).

DHS PRIVACY OFFICE

2015 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 (Privacy Office or Office) is the first statutorily mandated privacy office in the Federal Government, as set forth in Section 222 of the Homeland Security Act.[13] Its mission is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities while supporting the Department's mission to protect the homeland.

The Homeland Security Act expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[14] DHS exercises this authority in connection with the programs discussed in this report, all of which have been reviewed by the Chief Privacy Officer.

The DHS Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974[15] the E-Government Act of 2002[16] 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."[17]

The DHS Privacy Office implements the Chief Privacy Officer's authorities through privacy compliance policies and procedures, which are based on a set of eight Fair Information Practice Principles (FIPPs) rooted in the tenets of the Privacy Act. The FIPPs serve as DHS's core privacy framework. 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* (December 29, 2008)[18] and in Department-wide directives including, most recently, Directive 047-01, *Privacy Policy and Compliance* (July 7, 2011).[19] The FIPPs govern the appropriate collection, maintenance, use, and dissemination of

---

[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 of 2007 provided the Chief Privacy Officer with 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 2015 Annual Report to Congress*, available at: http://www.dhs.gov/sites/default/files/publications/dhsprivacyoffice2015annualreport-final-11102015.pdf

[14] 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).

[15] 5 U.S.C. § 552a.

[16] 44 U.S.C. § 3501 note.

[17] 6 U.S.C. § 142(a)(1).

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

[19] 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

Personally Identifiable Information (PII) at the Department in fulfilment of the Department's mission to preserve, protect, and secure the homeland. The Office applies the FIPPs to the DHS activities that involve data mining.

DHS uses three mechanisms to assess and enforce privacy compliance for DHS activities that involve data mining: (1) the Privacy Threshold Analysis (PTA);[20] (2) the Privacy Impact Assessment (PIA);[21] and (3) the System of Records Notice (SORN).[22] Each of these documents has a distinct function in the DHS privacy compliance framework. Together, they promote transparency and demonstrate accountability.

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.[23] 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 Modernization Act of 2014 (FISMA)[24] to determine whether they maintain PII. The PIA process also provides the Office insight into technologies used or intended to be used by DHS. These oversight activities provide the Office opportunities to learn about proposed data mining activities and to engage program managers in discussions about potential privacy issues.

The DHS Privacy Office has worked closely with the relevant DHS Components to ensure that privacy compliance documentation required for each program described in this report is current. 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 2014 DHS Data Mining Report,[25] the DHS Privacy Office discussed the following Departmental programs that engage in data mining, as defined by the Act:

---

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.

[20] The DHS privacy compliance process begins with a PTA, a required document that serves as the official determination by our office as to whether a Department program or system has privacy implications, and if additional privacy compliance documentation is required, such as a Privacy Impact Assessment (PIA) and System of Records Notice (SORN). Additional information concerning PTAs is available at: http://www.dhs.gov/compliance

[21] The E-Government Act mandates PIAs for all federal agencies when there are new electronic collections of, or new technologies applied to, PII. 44 U.S.C. § 3501 note. 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).

[23] The DHS Privacy Office reviews all major DHS IT programs on an annual basis, prior to submission to OMB for inclusion in the President's annual budget. *See* Office of Mgmt. & Budget, Executive Office of the President, OMB Circular No. A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, available at http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s300.pdf.

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

[25] 2014 DHS Data Mining Report available at: http://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf

(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 FALCON 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 section of the 2015 report presents complete descriptions of these programs together with updates on modifications, additions, and other developments that have occurred in the current reporting year.

A. Automated Targeting System (ATS)

1. 2015 Program Update

a) Non-Immigrant and Immigrant Visa Applications

As described in the 2012 ATS PIA,[26] 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 vetting. ATS-UPAX vets the visa application and provides a response to the DoS's Consular Consolidated Database (CCD)[27] 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 research, 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), 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[28] system for further investigation and possible enforcement

---

[26] The ATS PIA is available at: http://www.dhs.gov/privacy-impact-assessments.

[27] The CCD PIA is available at: https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf

[28] LeadTrac is an immigration status violator database that the Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit at ICE uses 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

action. In addition to prioritizing overstay leads, ATS is also used to vet overstay candidates received from the Arrival and Departure Information System (ADIS)[29] to identify potential additional information on visa overstay candidates based on supporting data available from other source systems through ATS, i.e., border crossing information (derived from the Border Crossing Information (BCI) system), Form I-94 Notice of Arrival/Departure records (derived from the Non-immigrant Information System (NIIS)), and data from the DHS Student Exchange Visitor Information System (SEVIS).[30]

As with the Phase 2 Pilot, discussed in DHS's 2013 and 2014 Data Mining Reports,[31] 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. In January 2014, ADIS transitioned from the Office of Biometric Identity Management (OBIM) in the DHS National Protection and Programs Directorate to CBP.[32] 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 activities are covered by PIAs for ATS,[33] the US-VISIT Technical Reconciliation Analysis Classification System,[34] and Overstay Vetting.[35]

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

---

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 PIA is available at: http://www.dhs.gov/privacy-impact-assessments.

[29] The PIA for ADIS is available at: http://www.dhs.gov/privacy-impact-assessments and the SORN for ADIS is available at: http://www.gpo.gov/fdsys/pkg/FR-2013-05-28/html/2013-12390.htm. The ATS PIA and the Overstay Vetting Pilot PIA, which also address this activity, are available at: http://www.dhs.gov/privacy-impact-assessments.

[30] The PIA for SEVIS is available at: http://www.dhs.gov/privacy-impact-assessments and the SORN for SEVIS is available at: http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm.

[31] 2013 Data Mining Report is available at: http://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf . The 2014 Data Mining Report is available at: http://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf

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

[33] The ATS PIA is available at: http://www.dhs.gov/privacy-impact-assessments.

[34] *See* DHS/NPPD/USVISIT/PIA-004 available 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.

[35] 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/privacy-impact-assessments.

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.[36]

c) Trusted Traveler Vetting

The vetting process for the Trusted Traveler Programs has evolved from CBP's legacy Vetting Center Module (VCM) to the ATS vetting process. Previously, CBP's VCM performed a series of system queries to gather data on Trusted Traveler Program applicants. CBP Officers analyzed and assessed this data to be utilized during the enrollment interview. The ATS Trusted Traveler Vetting Program is a modernized version of VCM.

On May 4, 2015, ATS Trusted Traveler Vetting Program capabilities were deployed to a CBP Vetting Center. ATS provides improved vetting algorithms, which are designed to assist in identifying more refined matches to derogatory records. The results of the vetting analysis provide a consolidated view of the applicant's information, derogatory matches, as well as other system checks. In November 2015, the ATS Trusted Traveler Vetting capabilities included a new grouping of Trusted Traveler applications that are marked as candidates for Auto-Conditional approval if certain conditions are met in the automated risk assessment process. At the time of this report, the information derived from these new capabilities is being used for testing and evaluation purposes only; these applications are not currently auto-conditionally approved. This testing and evaluation period will provide valuable data to determine if, or when, the automated process will occur. Once this process is reviewed and refined to sufficiently meet CBP requirements, ATS-UPAX will begin to auto-conditionally approve Trusted Traveler applicants, who will be referred directly to the Enrollment Centers for interview. This process is expected to reduce the workload for the CBP Vetting Center. Full transition to vetting of Trusted Traveler applicants in the ATS platform is expected by the second quarter of FY2016.

The legal authorities for the ATS Trusted Traveler Vetting include: Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, 8 U.S.C. § 1365b; Section 215 of the Immigration and Nationality Act, as amended, 8 U.S.C. § 1185; Section 402 of the Homeland Security Act of 2002, as amended, 6 U.S.C. § 202; Section 404 of the EBSVERA, 8 U.S.C. § 1753; and Section 433 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1433; 8 C.F.R. Parts 103 and 235.

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

---

[36] A complete list of authorities is included in the PIA for the Overstay Vetting Pilot, available at: http://www.dhs.gov/privacy-impact-assessments,

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. This enhanced program became operational 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.[37]

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 ongoing 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 co-travelers identified 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.[38]

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 sought to expand the success of Phase 1 by including additional information in the common dashboard display for both TSA and CBP. This information includes: 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

---

[37] The PIA for Watchkeeper is available at: http://www.dhs.gov/privacy-impact-assessments.
[38] The ATS PIA is available at: http://www.dhs.gov/privacy-impact-assessments.

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.[39]

These enhancements build upon the information sharing efforts between Secure Flight and ATS discussed DHS's 2013 and 2014 Data Mining 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 December 8, 2014.[40] 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).

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 and 2014 Data Mining Reports,[41] using existing CBP data collections and ATS-N to identify pre-departure air cargo that may pose a threat to aviation security. In July 2015, CBP extended the pilot through July 26, 2016.[42] 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 owns and manages 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

---

[39] The ATS PIA Update is available at: http://www.dhs.gov/privacy-impact-assessments.

[40] The Secure Flight PIA is available at: http://www.dhs.gov/privacy-impact-assessments.

[41] 2013 Data Mining Report is available at: http://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf . The 2014 Data Mining Report is available at: http://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf

[42] Extension of the Air Cargo Advance Screening (ACAS) Pilot Program and Reopening of Application Period for Participation, 80 Fed. Reg. 44360 (July 27, 2015), available at: https://www.federalregister.gov/articles/2015/07/27/2015-18287/extension-of-the-air-cargo-advance-screening-acas-pilot-program-and-reopening-of-application-period.

also uses ATS to identify other potential violations of U.S. laws that CBP enforces at the border under its authorities. 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,[43] imports, passengers and crew (airline passengers and crew on international flights, and passengers and crew on international sea carriers), private vehicles and travelers crossing at land borders, and a workspace to support the creation and retention of analytical reports. This report discusses 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).

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, or persons who may be importing or exporting merchandise in violation of United States law. ATS was originally designed as a rules-based program to identify such cargo and did not apply to travelers. ATS-N and ATS-AT[44] became operational in 1997. ATS-P (now referred to as ATS-UPAX)[45] became operational in 1999 and is now even more 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).[46]

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

---

[43] At the time of this report, CBP maintains the export targeting functionality 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 EIS PIA will be conducted to address these updates in greater detail.

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

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

[46] 49 U.S.C. § 44909. The regulations implementing ATSA are codified at 19 C.F.R. § 122.49d.

Nonimmigrant Information System (NIIS), BCI, ICE's SEVIS, and TECS.[47] TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[48] 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.

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 source system. Access to this functionality of ATS is restricted by existing technical security and privacy safeguards associated with the source systems.

A large number of rules are included in the ATS modules, so CBP Officers can analyze sophisticated concepts of business activity which in turn can help identify potentially suspicious behavior. The ATS rules are constantly evolving to meet new threats and be more effective. When evaluating risk, ATS is designed to apply 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.

---

[47] PIAs for these programs can be found at: http://www.dhs.gov/privacy-impact-assessments.

[48] 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 established the TSC pursuant to Homeland Security Presidential Directive 6 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.

The functionality of ATS-AT was modernized when the AES system was re-engineered and deployed by CBP. AES aids CBP officers in identifying export shipments 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 or departure from 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 automated results.

The SAFE Port Act requires CBP to use or investigate the use of advanced algorithms in support of its mission.[49] To that end, as discussed in previous DHS Data Mining Reports, CBP established an Advanced Targeting Initiative, which employs the development of data mining, machine learning,[50] 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 trade 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

---

[49] 6 U.S.C. §§ 901 *et seq.*

[50] 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.

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 the CBP Office of Intelligence 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,[51] 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 or persons and initially collected in DHS/CBP source systems (e.g., ACE, ACS) in accordance with U.S. legal 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.

ATS-N and ATS-AT use the information from source systems 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, consignees, 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.[52] 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 indicate 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

---

[51] 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.
[52] 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.

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 proven 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 may apply additional scrutiny to such referrals; including opening the cargo container to remove and inspect its contents. During the exam, CBP officers may detain, seize, forfeit, or deny entry of commodities that are contraband or otherwise not admissible. For example, in September 2015, a foreign customs authority seized 240 kilos (528 pounds) of cocaine based on a referral by NTC. The shipment in question originated from South America and was en route to a European country. The foreign customs authority conducted a physical exam of two sea containers and discovered the narcotics in duffel bags on board. In another instance, in March 2015, the NTC identified and referred three shipments that were believed to contain contraband. The shipments were on three separate sea containers arriving in North America from South America. NTC contacted authorities who conducted a physical examination of the shipments. A total of 315.46 kilos (695.47 pounds) of cocaine were discovered and subsequently seized.

Additionally, NTC identified and referred a non-containerized sea shipment. The shipment was scheduled to export from the United States and was destined for overseas. CBP examined the shipment and discovered merchandise that the exporter did not have proper authorization to ship. The exporter submitted an authorization request to the Office of Foreign Assets Control, but was denied because not all parties in the prospective transaction were fully identified. Further collaboration with ICE revealed that the final destination of the shipment was Iran. In September 2015, CBP seized the shipment for violating the International Emergency Economic Powers Act.[53]

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.[54] 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[55]

---

[53] 50 U.S.C. §§ 1701 *et seq.*
[54] *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.
[55] 22 U.S.C. §§ 5201 *et seq.*

and the 1996 Clinger-Cohen Act.[56] The risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.[57]

b) ATS-Unified Passenger Module (ATS-UPAX, formerly ATS-Passenger (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 at the CBP NTC to evaluate passengers and crew members prior to their arrival to or departure from the United States. ATS-UPAX is a technology refresh of the ATS-P Module and 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 person 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 CBPs' System Engineering Life Cycle methodology[58] 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 through ATS, and apply risk-based rules based on CBP officer expertise, 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 links and sign-on protocols employ the underlying sharing agreements that support the same 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.

---

[56] 40 U.S.C. §§ 1401 *et seq.*

[57] 6 U.S.C. § 912(b).[58] 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.

[58] 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.

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 available through ATS 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 available through 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 automated results of the data mining of information available through 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: 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 seeking authorization to travel under the Visa Waiver Program (VWP)[59]; the DHS Suspect and Violator Indices (SAVI); and the DoS visa databases. ATS-UPAX also relies upon PNR information from air carriers, BCI crossing data, seizure data, Report of International Transportation of Currency or Monetary Instrument Report (CMIR) data,[60] and information from the TSDB and TECS.

---

[59] 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.

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

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 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, made recommendations to carriers not to board such persons. 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 subject who was involved in terrorism financing. Based on the research conducted by the NTC, the subject was nominated to the TSDB and the indivial's visa was revoked by the DoS. Subsequently, the subject attempted to travel to the United States, and CBP contacted the air carrier and advised that the subject would likely be found inadmissable to the United States if permitted to travel. The subject was denied boarding by the air carrier. In another instance, CBP, working at the NTC in conjunction with a United States Marshals Service (USMS) Liaison, identified a U.S. Citizen who was living abroad and was a USMS Top 15 fugitive for sexual abuse of minors. Using ATS-UPAX, CBP was able to provide information to USMS to assist in locating the fugitive, which subsequently led to his arrest.

There are many instances in which rules developed by CBP headquarters or field personnel lead to significant arrests and/or seizures. For instance, in 2015, CBP referred an individual who was arriving from one country via another country for further inspection. The passenger stated he was visiting his ailing relative, and had one checked bag in his possession. CBP officers inspected the suitcase, including removing all contents. Upon feeling the weight of the empty piece of luggage, which was unusually heavy, the luggage was probed revealing a white powdery substance that tested positive for cocaine. The passenger was arrested for the importation of narcotics.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.[61] 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

---

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

customs purposes. The information collected is authorized pursuant to the EBSVERA,[62] ATSA, IRTPA, the INA, and the Tariff Act of 1930, as amended.[63] 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 between the ports of entry 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 or persons 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 updated annually, at a minimum, through the use of a predictive model to help identify people and vehicles with an increased risk of transporting certain types of illegal drugs. 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 travelers or supporting information for the clearance and admission of the vehicle and its travelers.

---

[62] 8 U.S.C. § 1721
[63] 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.

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

iii. Data Sources

ATS-L uses and relies upon available information from the following systems to assist in the development of the risk-based rules discussed above: NIIS, ESTA, SAVI, and DoS visa. ATS-L also relies upon TECS 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 person 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 a 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 and agents 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 and agents are acting upon the most up to date information. For example, in October 2015, ATS-L alerted CBP Officers to a vehicle bearing California plates and the vehicle occupants, two United States citizens, were referred to secondary for inspection. During secondary inspection, a canine alerted to the undercarriage of the vehicle. An inspection of the vehicle found tampering to the sending unit underneath the back passenger's seat. The cover was removed which revealed packages in the gas tank. A field test showed the substance in the packages was methamphetamine. The driver was arrested for the importation of narcotics. A total of thirty-two (32) packages of methamphetamine weighing 36.61 lbs. were seized.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information about vehicles and their occupants prior to entering the United States.[64] As part of this inspection and examination process, all vehicles and persons 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 persons (which they may be required to present to a CBP officer upon arrival in the United States), on the vehicle's license plate, and in 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 for ATS on September 16, 2014,[65] and updated the 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 agents 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.[66] ATS supports, but does not replace, the decision-making responsibility of CBP officers, agents, 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, U.S. Food and Drug

---

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

[65] ATS PIA Update is available at: http://www.dhs.gov/privacy-impact-assessments.

[66] TSA, ICE, USCIS, USCG 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.

Administration, U.S. Fish and Wildlife Service, and the National Marine Fisheries Service. Each member of the CTAC 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.[67]

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 CBPs' 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.[68] 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.[69]

Under the ATS PIA and SORN, and as a matter of DHS policy, CBP permits any subject of PNR or his or her representative to make administrative requests for access and amendment of the PNR. Procedures for individuals to request access to PNR within ATS 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 request 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

---

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

[68] 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.

[69] DHS TRIP can be accessed at: http://www.dhs.gov/dhs-trip.

additional means of access to PII held in source systems.[70] Privacy Act and FOIA requests for access to information for which ATS is the source system are directed to CBP.[71]

ATS underwent the Security Authorization process in accordance with DHS and CBP policy and obtained its initial Security Authorization on June 16, 2006. ATS also completed a Security Risk Assessment on March 28, 2006, in compliance with FISMA, OMB policy, and National Institute of Standards and Technology guidance. The ATS Security Authorization and Security Risk Assessment were subsequently updated and are valid until January 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 approved computer systems, including ATS. As a condition precedent to obtaining access to ATS, all system users 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.[72] The retention period for PNR, which is contained only in ATS-UPAX, is subject to the following further access restrictions and masking requirements: ATS-UPAX users with PNR access 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 is transferred to a dormant database for a period of up to ten years. PNR in dormant status is subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be unmasked in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk.[73]

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

---

[70] 5 U.S.C. § 552.

[71] Requests may be submitted by mail to FOIA Officer, 1300 Pennsylvania Avenue, NW, Room 3.3D, Washington, D.C. 20229.

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

[73] 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. 2015 Program Update

The 2014 Data Mining Report described the Cross Domain Capabilities (CDC) Pilot, enabling analysts to view both Secret and Sensitive But Unclassified (SBU) data on the same screens, and allowing for a more effective information flow between security domains. This CDC Pilot was successfully concluded in 2015.

AFI has become 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. [74]

The addition of select legacy IFS datasets to AFI, and expansion to additional DHS users, will be included in a PIA update for AFI.

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[75] developed in connection with the above purposes with DHS employees who have a need to know in the performance of their official duties and who have appropriate clearances or permissions, or externally pursuant to routine uses in the AFI SORN.

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

---

[74] The PIA for AFI is available at: http://www.dhs.gov/privacy-impact-assessments. 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 Fed. Reg. 33753 (June 7, 2012).

[75] "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.

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 assist in identifying potential law enforcement or security risks.

AFI provides a set of analytical tools that include advanced search capabilities into existing DHS data sources, and federated queries to other federal agency sources and commercial data aggregators, to allow analysts to search several databases simultaneously. AFI tools 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"[76] 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 DoS, DOJ/FBI, and commercial data aggregators that are already available to DHS users. AFI tracks where AFI analysts search and routinely audits these records. AFI analysts use data that is available from commercial data aggregators to complement or clarify the data to which they have access within DHS. AFI provides a suite of tools that assist analysts in detecting trends, patterns, and emerging threats, and in identifying non-obvious relationships, using the information maintained in the index and made accessible through the federated query.

AFI also serves as a workspace that allows AFI analysts to create finished intelligence products, to maintain and track projects throughout their lifecycle from inception to finished intelligence product or from RFI to response, and to share finished intelligence products either within DHS or externally through regular law enforcement and intelligence channels to authorized users with a need to know, pursuant to routine uses in the AFI SORN.[77]

---

[76] 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.

[77] A detailed description of the processes leading to finished intelligence products and RFI responses is included in the PIA for AFI available at: http://www.dhs.gov/privacy-impact-assessments.

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 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, collaboration, analysis, summarization, and reporting capabilities. These include text analysis, link analysis, and geospatial analysis.

Specific types of analysis include:

- *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.

- *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.

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. In all situations, research developed or reports created by AFI analysts are subject to supervisory review.

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, 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:

- o 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);

- o 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);[78] National Security Entry-Exit Program information from ENFORCE; SEVIS information; and seizure information from the Seized Asset and Case Tracking System);

- o 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 (EID)[79] detention data, ICE intelligence information reports, ICE intelligence products, ICE name trace, ICE significant event notification Detention and Removal Leads, and TECS Reports of Investigation).[80]

- *Other Government Agency Data*: AFI obtains imagery data from the National Geospatial-Intelligence Agency and obtains other government agency data to the extent available through ATS, such as identity and biographical information, wants and warrants, DMV data, and data from the TSDB.[81]

- *Commercial Data*: AFI collects identity and imagery data from several commercial data aggregators so that DHS AFI analysts can cross-reference that information with the information contained in DHS-owned systems. Commercial data aggregators include sources available by subscription only (e.g., Lexis-Nexis) 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

---

[78] The SORN for ENFORCE is available at: https://www.gpo.gov/fdsys/pkg/FR-2015-04-30/html/2015-09615.htm
[79] The PIA for EID is available at: http://www.dhs.gov/privacy-impact-assessments.
[80] ICE and the Privacy Office issued a PIA for IFS on November 17, 2008. The IFS PIA is available at: http://www.dhs.gov/privacy-impact-assessments.
[81] A more complete discussion of other government agency data that may be accessed through ATS can be found in the ATS PIA available at: http://www.dhs.gov/privacy-impact-assessments.

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 continues to assist with improved information sharing amongst participating DHS components For example, ICE personnel, assigned to the Department of Defense (DoD), came across a CBP intelligence report while conducting research in AFI. AFI provided a summary of the intelligence report and contact information for the CBP author. ICE personnel were able to determine, based on the summary of the intelligence report, that the full report would be pertinent to work with the DoD.

Using the contact information provided in AFI, the agent was able to request the full report for internal consumption. This evolved into an additional request and subsequent approval for further dissemination of the report to federal partners within DoD and the Intelligence Community.

In another instance, AFI users were able to enhance CBP's understanding of individuals identified on the Department of Treasury's list of Specially Designated Nationals (SDN). By simultaneously searching across multiple CBP data sources, analysts were able to use AFI's capabilities and CBP data holdings to identify individuals and companies operating in the same manner and locations as the SDNs. These individuals and companies were then identified to CBP's National Targeting Center for further analysis.

6. Laws and Regulations

Numerous authorities mandate that DHS and CBP provide border security and safeguard the homeland, including: Title II of the Homeland Security Act (Pub. L. 107-296), as amended by IRTPA; the Tariff Act of 1930, as amended; the INA (8 U.S.C. §§ 1101 *et seq.*); the 9/11

Commission Act (Pub. L. 110-53); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132); the SAFE Port Act; ATSA; and 6 U.S.C. § 202.

7.   Privacy Impact and Privacy Protections

CBP does not use the information in AFI to make unevaluated automated decisions about individuals. Given the breadth of the data available to AFI users, CBP has built extensive privacy protections into the structure and governance of AFI.[82] AFI itself 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.[83]

AFI continues to be 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, Field Operations, Border Patrol, Air & Marine, Chief Counsel, Internal Affairs, Information Technology, and Privacy and Diversity, who review requested changes to the system on a quarterly basis and determine whether additional input is required. The governance board directs the development of new aspects of AFI, and reviews and approves new or changed uses of AFI, new or updated user types, and new or expanded data to be made available in or through AFI. As an added layer of oversight, the DHS Privacy Office conducted and published a PCR for AFI on December 19, 2014.[84]

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 also maintained 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.[85] 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 annual 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 privileges to all CBP computer systems, including AFI.

---

[82] The PIA for AFI includes a more complete description of these protections and is available at: http://www.dhs.gov/privacy-impact-assessments.

[83] The PIA for AFI is available at: http://www.dhs.gov/privacy-impact-assessments. 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 Fed. Reg. 33753 (June 7, 2012).

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

[85] 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.

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.

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

Because 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.[86]

---

[86] 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 if it is determined that 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

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 for records contained in AFI. 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. 2015 Program Update

During the 2015 reporting period, ICE made no modifications or updates to FALCON-DARTTS, which resides in the ICE Homeland Security Investigations (HSI) FALCON environment. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other government applications and systems, with appropriate user access restrictions and robust user auditing controls.[87]

ICE published the PIA for FALCON-DARTTS on January 16, 2014[88] 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.[89] On December 1, 2014, ICE republished the Trade Transparency Analysis and Research (TTAR) SORN, which applies to FALCON-DARTTS.[90]

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

---

accordance with procedures published in the applicable SORN. Requests may be submitted to U.S. Customs and Border Protection, FOIA Officer, 1300 Pennsylvania Avenue, NW, Room 3.3D, Washington, D.C. 20229. Additional information on submitting FOIA and Privacy Act requests is included in the PIA available at: http://www.dhs.gov/privacy-impact-assessments.

[87] 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, available at: http://www.dhs.gov/privacy-impact-assessments.

[88] *See* DHS/ICE/PIA-038 FALCON-DARTTS, January 16, 2014, available at: http://www.dhs.gov/privacy-impact-assessments.

[89] *See* DHS/ICE/PIA-032a FALCON-SA, January 16, 2014, available at: http://www.dhs.gov/privacy-impact-assessments.

[90] *See* DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, December 1, 2014, available at: 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*.

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 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.[91] 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

---

[91] 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.

data storage environment.[92] 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 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,[93] link analysis, and charting and graphing tools that use proprietary statistical algorithms.[94] It also allows non-technical users with investigative experience to analyze large quantities of data and rapidly identify problem areas. The program makes it easier 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

---

[92] 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.

[93] 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.

[94] 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.

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").[95] ICE receives data from the sources listed below via CD-ROM, external storage devices, or electronic data transfers and loads the data into FALCON-DARTTS and the FALCON general data storage environment. The agencies that provide FALCON-DARTTS with trade data collect any PII directly from individuals or enterprises completing import-export electronic or paper forms.[96] 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.[97] 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

---

[95] 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.

[96] 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.

[97] 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.

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 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,[98] 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.[99]

---

[98] 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.

[99] 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.

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.

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 El Paso used FALCON-DARTTS analytics in an investigation related to the unauthorized engagement in wholesale activities with Mexican customers who illegally export merchandise into Mexico, circumventing U.S. and Mexican laws. The U.S. company structured funds into multiple banks in the El Paso area to avoid reporting requirements. The HSI investigation revealed that the U.S. company was not authorized to engage in wholesale activities with merchandise purchased directly from brands such as NIKE, PUMA, and CONVERSE. This activity was indicative of Trade Based Money Laundering (TBML) via a Black Market Peso Exchange (BMPE) scheme which entails the exchange of Mexican pesos with U.S. dollars to purchase commercial goods and export into Mexico contrary to law. In November 2014, the Western District of Texas Grand Jury issued an indictment of the company's owner and several associates for violations of 18 U.S.C. § 554 (Smuggling goods

from the United States); 18 U.S.C. § 1956(h) (Conspiracy to Launder Monetary Instruments); 18 U.S.C. § 1957 (Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity); 18 U.S.C. § 1349 (Conspiracy to Commit Mail and Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); and 18 U.S.C. § 1343 (Wire Fraud).

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,[100] the Trade Secrets Act,[101] and the BSA.[102]

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.[103] FALCON-

---

[100] 5 U.S.C. § 552a.

[101] 18 U.S.C. § 1905.

[102] 31 U.S.C. § 5311.

[103] 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 at 77 Fed Reg. 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 Fed. Reg. 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 Fed. Reg. 77759 (Dec. 19, 2008), available at: http://www.gpo.gov/fdsys/pkg/FR-2008-12-

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.[104]

All raw data analyzed by FALCON-DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority. Therefore, FALCON-DARTTS relies on the systems and/or programs performing the original collection to provide accurate data. The majority of the raw data used by FALCON-DARTTS is accurate because the data was collected directly from the individual or entity to whom the data pertains. Due to the law enforcement context in which FALCON-DARTTS is used, however, there are often significant impediments to directly verifying the accuracy of information with the individual to whom the specific information pertains.[105] 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.[106]

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

19/html/E8-29801.htm), and TECS (DHS/CBP-011) (73 Fed. Reg. 77778 (Dec. 19, 2008), available at: http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm).

[104] FALCON-DARTTS is covered by the SORN for the ICE Trade Transparency and Analysis Research (TTAR) system of records, 79 Fed. Reg. 71112 (Dec. 1, 2014) available at: http://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm.

[105] 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.

[106] For more information on these controls, auditing, and accountability, see the FALCON-SA PIA available at: http://www.dhs.gov/privacy-impact-assessments.

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 BSA 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.

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.   2015 Program Update

Since the system's launch in November 2014, ICE has made no modifications or updates to FALCON-Roadrunner. 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 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.[107]

---

[107] In February 2012, ICE deployed the first module of FALCON with the launch of 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* the FALCON-SA PIA available at: http://www.dhs.gov/privacy-impact-assessments.

ICE published the FALCON-Roadrunner PIA on November 12, 2014.[108] On December 1, 2014, ICE republished the TTAR SORN to expand its coverage to FALCON-Roadrunner.[109] Lastly, ICE is in the process of updating the FALCON-SA PIA Appendix to capture the immigration, law enforcement, and publicly available FALCON-Roadrunner data that is being stored in the FALCON environment and made accessible to additional users through FALCON-SA's user interface, and plans to publish an updated PIA in 2016.

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;[110] 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

---

[108] FALCON-Roadrunner PIA available at: http://www.dhs.gov/privacy-impact-assessments.

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

[110] 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.

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.

3.   Technology and Methodology

FALCON-Roadrunner allows users[111] 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.

---

[111] 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.'

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.
> (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[112] that CBP collects from individuals and entities exporting merchandise from the United States.

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[113] and the publicly available consolidated U.S. export screening lists of the U.S. Department of Commerce, State, and Treasury.[114] 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.[115]

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.[116]

---

[112] 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* the Export Information System (EIS) PIA, available at: http://www.dhs.gov/privacy-impact-assessments.

[113] 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.

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

[115] 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.

[116] *See* TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative and TECS System: CBP Primary and Secondary Processing PIAs, available at: http://www.dhs.gov/privacy-impact-assessments. *See also* DHS/CBP-011 U.S. Customs and Border Protection TECS SORN, 73 Fed. Reg. 77778 (Dec. 19, 2008), available at: http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

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.[117]

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

FALCON-Roadrunner became operational under a limited pilot established at the HSI Assistant Special Agent in Charge office located in Sterling, Virginia. Since January 2015, analysts working under the program have generated 26 Special Agent in Charge (SAC) Area of Responsibility (AOR) reports and 44 Attaché AOR reports. These reports are designed to enhance situational awareness of export activity in the respective AORs. To date, the program has fielded 43 analytic support requests in support of nine active criminal investigations. The program has sent 11 investigative lead packages to the HSI Attaché Singapore and seven investigative lead packages to HSI SAC offices in Boston, Washington D.C., Milwaukee, and New Haven. The lead packages have enhanced one ongoing investigation, led to the opening of two new criminal investigations, and resulted in the seizure of high end nuclear filters destined for Iran and a separate seizure of a vehicle containing weapons destined for Lebanon.

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. Specifically, 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.

---

[117] Visa Security Program Tracking System-Network PIA available at: http://www.dhs.gov/privacy-impact-assessments and Visa Security Program Records SORN, 74 Fed. Reg. 50228 (Sept. 30, 2009), available at http://www.gpo.gov/fdsys/pkg/FR-2009-09-30/html/E9-23522.htm.

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 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.[118] 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.[119]

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

---

[118] 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 Fed. Reg. 77759 (Dec. 19, 2008), available at: https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29801.htm; DHS/CBP-001 Automated Commercial Environment/International Trade Data System (ACE/ITDS) SORN, 71 Fed. Reg. 3109 (Jan. 19. 2006), available at: https://www.gpo.gov/fdsys/pkg/FR-2006-01-19/html/E6-511.htm ; DHS/CBP-011 TECS SORN, 73 Fed. Reg. 77778 (Dec. 19, 2008), available at: https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm; DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, 79 Fed. Reg. 71112 (Dec. 1, 2014), available at: https://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm; DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN, 75 Fed. Reg. 9233 (Mar. 1, 2010), available at: https://www.gpo.gov/fdsys/pkg/FR-2010-03-01/html/2010-4102.htm; and DHS/ICE-012 Visa Security Program Records SORN, 74 Fed. Reg. 50228 (Sept. 30, 2009), available at: at http://www.gpo.gov/fdsys/pkg/FR-2009-09-30/html/E9-23522.htm.

[119] FALCON-Roadrunner is covered by by the following SORN: DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN, 79 Fed. Reg. 71112, (Dec. 1, 2014) available at: https://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm.

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 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.[120]

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.   2015 Program Update

DHS continues to mature its Department-wide big data program, the DHS Data Framework.[121] In April 2015, the Framework entered its Initial Operational Capability. The current iteration of the Framework includes Neptune,[122] an unclassified platform, and Cerberus,[123] a classified platform. To ensure appropriate technical and policy governance of the program—including the incorporation of robust privacy, civil rights, and civil liberties protections—DHS is deploying

---

[120] FALCON-SA PIA available at: http://www.dhs.gov/privacy-impact-assessments.

[121] The April 2015 DHS Data Framework PIA is available at: http://www.dhs.gov/privacy-impact-assessments.

[122] Neptune PIAs are available at: http://www.dhs.gov/privacy-impact-assessments.

[123] Cerberus PIAs are available at: http://www.dhs.gov/privacy-impact-assessments.

the Framework in an iterative fashion. Below is a summary of the Data Framework phases to date:

- *Pilot Phase:* Between November 2013 and August 2014, DHS deployed a Framework Pilot phase to test the mission utility, technical feasibility, and policy protections of the Framework in a non-operational context.[124]

- *Limited Production Capability Phase:* Between August 2014 and April 2015, DHS deployed a Limited Production Capability to further test the Framework's capabilities within a controlled operational context.[125]

- *Initial Operational Capability Phase:* Beginning in April 2015, DHS entered an Initial Operational Capability phase. Initially, the Framework's uses, users, and capabilities (i.e., the basic search functions) will remain the same as during the Limited Production Capability phase. However, during the Initial Operational Capability phase, the Framework will include new DHS data sets and may add new types of DHS users and new technical capabilities (e.g., increased data refresh capabilities) for use within a controlled operational context. The search and analytic capabilities continue to be limited to the three basic search functions deployed in the pilot/prototype and Limited Production Capability phase: person search, characteristic search, and trend search.

The Department's original plans were to ingest three to five data sets each year, with a total of 20 to 24 data sets added over the next several years. However, in January 2015, the Framework Program was directed to set a goal of 20 datasets in the Framework by the end of 2016. As of September 30, 2015, seven data sets have been approved for inclusion in the Initial Operational Capability. These data sets are identified in Appendix A[126] of the Framework PIA and include: ESTA; AFSP; SEVIS; APIS; Form I-94;[127] Passenger Name Record (PNR);[128] and Section 1367 Data Extracted from the Central Index System.[129] DHS will update Appendix A of the Framework PIA as new data sets are added.

---

[124] For more information about the Pilot phase, please see the following PIAs: DHS/ALL/PIA-046 DHS Data Framework,; DHS/ALL/PIA-046-1 Neptune Pilot; DHS/ALL/PIA-046-2 Common Entity Index Prototype; and DHS/ALL/PIA-046-3 Cerberus Pilot, available at: http://www.dhs.gov/privacy-impact-assessments.

[125] For more information about the Limited Production Capability phase, please see the following PIAs: DHS/ALL/PIA-046-1(a) Neptune Pilot; and DHS/ALL/PIA-046-3(a) Cerberus Pilot, available at: http://www.dhs.gov/privacy-impact-assessments.

[126] Appendix A is available at: http://www.dhs.gov/sites/default/files/publications/PIA%20DHS%20-%20Data%20Framework%20-%20IOC%20Appendix%20A%2020150930%20PRIV%20Final.pdf.

[127] The PIA for DHS/CBP/PIA-016 for Form I-94 Automation is available at: http://www.dhs.gov/privacy-impact-assessments.

[128] PNR information is covered by DHS/CBP/PIA-006(d) ATS-TSA/CBP Common Operating Picture Phase II, available at: http://www.dhs.gov/privacy-impact-assessments. The associated SORN is available at: https://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm

[129] The PIA for DHS/USCIS/PIA-009 Central Index System is available at: http://www.dhs.gov/privacy-impact-assessments. The associated SORN is available at: http://www.gpo.gov/fdsys/pkg/FR-2013-11-21/html/2013-27895.htm

During the Initial Operational Capability phase, the Framework will continue to rely on the source IT systems to notify the Framework of updates and corrections to the data sets. Updates and corrections to the data sets will be incorporated into the Framework with each data refresh. In August, the Framework completed development of its capability near-real-time data refresh. This significant addition decreases the delay between when updates or corrections are made in the source IT system and when those updates or corrections are presented to the users. At this time, not all source systems are capable of delivering data in near real time, so the limiting factor is the speed at which the source system can provide the data. Currently ESTA is the only system providing near-real-time data transfer. It still holds that any corrections or changes to the data will happen at the source IT system, and will be incorporated into the Data Framework by the Data Framework Program during the subsequent data refresh.

Until source systems establish a near real-time data refresh capability, DHS personnel must verify the data in the underlying source IT system. This extra step is a privacy protection that ensures data quality and an operational protection to ensure that DHS personnel are using accurate information in DHS operations.

During the Initial Operational Capability, DHS will expand the users of the Data Framework to the DHS Intelligence Enterprise. The uses will remain limited to counterterrorism, border security, and immigration. The DHS Intelligence Enterprise[130] consists of the intelligence offices of the following DHS Components:

- U.S. Customs and Border Protection;
- U.S. Immigration and Customs Enforcement;
- U.S. Citizenship and Immigration Services;
- U.S. Coast Guard;
- Transportation Security Administration;
- U.S. Secret Service; and
- Federal Emergency Management Agency.

The Department is establishing the DHS Data Framework Steering Group (DFSG), an executive steering committee, with a charter approved by the Secretary. The charter defines the mission, authority, membership, responsibilities, and operating principles for the DFSG. The mission of the DFSG is to provide effective governance, oversight, coordination, and direction to the Framework and all related projects and initiatives and to ensure its successful and timely delivery in compliance with all policy- and user-based requirements. In addition to DHS mission and technical representatives, the DFSG's membership includes "oversight offices," i.e., the Privacy Office, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel.

Active and continued enhancement of the governance structure is among the most significant changes that DHS is making to the Framework since the publication of the PIA for the Limited Production Capability phase. By design, the DFSG brings together expertise in a number of

---

[130] More information about the DHS Intelligence Enterprise is available at: http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission.

areas including mission operations, information technology, and oversight to ensure the Framework delivers mission capabilities while ensuring all legal, policy, technical, security, privacy, civil rights, and civil liberties protections and requirements are met.

Finally, to expedite its ability to meet a critical mission need, DHS created an interim data transfer process that foregoes some of the automated protections of the Framework, such as the enforcement of access control policies in the classified data lake. In lieu of automated access control policies, DHS is controlling access by creating accounts for approved users. DHS has a critical mission need to perform classified queries on its unclassified data in order to identify individuals supporting the terrorist activities of: (1) the Islamic State of Iraq and the Levant (ISIL), (2) al-Qa'ida in the Arabian Peninsula (AQAP), (3) al-Nusrah Front, (4) affiliated offshoots of these groups, or (5) individuals seeking to join the Syria-Iraq conflict (These individuals are often referred to as "foreign fighters" by the media and in public discourse.) The ability to perform classified searches of unclassified data for this uniquely time-sensitive purpose will allow DHS to better identify and track foreign fighters who may seek to travel from, to, or through the United States. This type of comparison is a long-standing mission need; however, the specific threat has shortened the timeframe in which DHS must meet the need. By foregoing the automated protections of the Framework, DHS will be able to expedite transfers of information from ESTA, APIS, Form I-94 records, and PNR directly from the unclassified DHS domain to the classified DHS domain.

Although the interim process deviates from the standard model of the Data Framework, DHS is pursuing this process under the auspices of the Data Framework in order to utilize aspects of the Framework's policies, governance, and transparency. Moreover, the interim solution will only continue until the standard model is capable of meeting the mission need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission needs in the long-term, and the Department will revert to the standard model once the technical capabilities are available. Consequently, regular development on the Framework will continue and will not be affected by the use of the interim process.

The DHS Privacy Office has been intensively involved in the development of these capabilities and in the 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 Framework as it becomes operational.

2.   Program Description

DHS developed the 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.

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.[131] 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 Framework is to provide a user the ability to search an amalgamation of data extracted from multiple DHS systems for a specific purpose and to view the information in a clear and accessible format. The Framework enables efficient and cost-effective searches across DHS databases in both classified and unclassified domains.

The 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 were tested to enable greater information sharing and comparison in support of operations and to build in greater privacy protections. The 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, SEVIS, and AFSP.

---

[131] *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.

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

- *CEI Prototype:* The CEI Prototype, also residing on the SBU/FOUO domain, received a subset of the tagged data from the Neptune Pilot and correlates data from across component datasets. The CEI Prototype tested 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 used data tags to test the third and fourth elements of the DHS Data Framework (context and dynamic access control, respectively).

- *Cerberus Pilot:* The Cerberus Pilot, residing in the Top Secret/Sensitive Compartmented Information (TS/SCI) domain, received all of the tagged data from the Neptune Pilot in a separate data repository known as Cerberus. The Cerberus Pilot tested 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 leveraged the data tags to test the context and dynamic access control elements of the DHS Data Framework. The Cerberus Pilot also tested the ability to perform simple and complex searches across different component datasets using different analytical tools.

During the pilot phase of the 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

As of November 24, 2015, seven data sets have been approved for inclusion in the Initial Operational Capability. These data sets are identified in Appendix A[132] of the Framework PIA and include: ESTA; AFSP; SEVIS; APIS; Form I-94; PNR; and Section 1367 Data Extracted from the Central Index System. The authorities and policies for each of these data sets are also applied in the Framework. For a high-level description of each data set in the Framework, please see Appendix A of the Framework PIA.

5. Efficacy

Based on the Framework's success to date, the Department moved from the limited production capability to an Initial Operational Capability for both the Neptune and Cerberus systems. During the Initial Operational Capability, DHS will add new DHS data sets and new users from the DHS Intelligence Enterprise. DHS will provide additional information in future Data Mining Reports on the efficacy of the Framework.

---

[132] Appendix A to the Framework PIA is available at: http://www.dhs.gov/sites/default/files/publications/PIA%20DHS%20-%20Data%20Framework%20-%20IOC%20Appendix%20A%2020150930%20PRIV%20Final.pdf.

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 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.

7. Privacy Impact and Privacy Protections

Robust privacy protections are the bedrock of the Framework. Accordingly, DHS performed in-depth privacy impact assessments of the Framework and its underlying components. Specifically, DHS has published privacy impact assessments for the DHS Data Framework itself,[133] Cerberus,[134] Neptune,[135] CEI,[136] and the Interim Process to Address an Emergent Threat.[137] The privacy protections for the 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 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 Framework's privacy impacts and protections, please see the relevant privacy impact assessments.[138]

IV. CONCLUSION

The DHS Privacy Office is pleased to provide the Congress its tenth 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 Privacy Office has

---

[133] DHS/ALL/PIA-046 DHS Data Framework. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments.

[134] DHS/ALL/PIA-046-3 Cerberus. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments.

[135] DHS/ALL/PIA-046-1 Neptune. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments.

[136] DHS/ALL/PIA-046-2 Common Entity Index. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments.

[137] DHS/ALL/PIA-051 DHS Data Framework – Interim Process to Address an Emergent Threat, available at: http://www.dhs.gov/privacy-impact-assessments.

[138] DHS/ALL/PIA-046 DHS Data Framework. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments; DHS/ALL/PIA-046-3 Cerberus. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments; DHS/ALL/PIA-046-1 Neptune. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments; DHS/ALL/PIA-046-2 Common Entity Index. Multiple iterations are available at: http://www.dhs.gov/privacy-impact-assessments.

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.

V. APPENDIX

Acronym List	
ACAS	Air Cargo Advance Screening
ACE	Automated Commercial Environment
ACS	Automated Commercial System
ADIS	Arrival and Departure Information System
AES	Automated Export System
AFI	Analytical Framework for Intelligence
AFSP	Alien Flight Student Program
AMS	Automated Manifest System
APIS	Advance Passenger Information System
ATO	Authorization to Operate
ATS	Automated Targeting System
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 Report
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 Database
ESTA	Electronic System for Travel Authorization
FALCON-SA	FALCON Search & Analysis

Acronym List	
FBI	Federal Bureau of Investigation
FinCEN	Department of the Treasury Financial Crimes Enforcement Network
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HSI	ICE Homeland Security Investigations
I&A	DHS Office of Intelligence and Analysis
ICE	U.S. Immigration and Customs Enforcement
IFS	Intelligence Fusion System
INA	Immigration and Nationality Act
IOC	Interagency Operations Center
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IT	Information Technology
LES	Law Enforcement Sensitive
MSB	Money Services Business
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NIIS	Nonimmigrant Information System
NTC	National Targeting Center
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
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

Acronym List	
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