

Privacy Office

# 2016 Data Mining Report to Congress

April 2017



**Homeland  
Security**

## FOREWORD

*April 2017*

I am pleased to present the Department of Homeland Security's (DHS) 2016 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 eleventh comprehensive DHS Data Mining Report and the ninth report prepared pursuant to the Act. Three annexes to this report, which include Law Enforcement Sensitive information, Sensitive Security Information, and classified 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 Michael Pence**

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 Claire McCaskill**

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 Dianne Feinstein**

Ranking Member, U.S. Senate Committee on the Judiciary

**The Honorable Richard Burr**

Chairman, U.S. Senate Select Committee on Intelligence

**The Honorable Mark Warner**

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,



Jonathan R. Cantor  
Acting 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).<sup>1</sup> 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 2015 DHS Data Mining Report,<sup>2</sup> the DHS Privacy Office discussed the following Departmental programs that engage in data mining, as defined by the Act:

- The Automated Targeting System (ATS), which is administered by U.S. Customs and Border Protection (CBP) and includes modules for inbound (ATS-N) and outbound (ATS-AT) cargo, land border crossings (ATS-L), and passengers (ATS-P);
- The Analytical Framework for Intelligence (AFI), which is administered by CBP;
- The FALCON Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by U.S. Immigration and Customs Enforcement (ICE);
- The FALCON-Roadrunner system, which is administered by ICE; and
- The DHS Data Framework, which is a DHS-wide initiative.

This year's report, covering the period January 1, 2016 through December 31, 2016, provides updates on modifications, additions, and other developments to the above referenced programs. In addition, the DHS Privacy Office identified two additional Departmental programs that engage in data mining, as defined by the Act:

- The SOCRATES Pilot Program, which is administered by CBP; and
- The Fraud Detection and National Security – Data System (FDNS-DS), which is administered by the United States Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security Directorate (FDNS).

DHS is also providing three annexes to this report, which include Law Enforcement Sensitive information, Sensitive Security Information, and classified information, respectively, to Congress as required by the Act.

The Homeland Security Act of 2002 expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.<sup>3</sup> DHS exercises this authority with

<sup>1</sup> 42 U.S.C. § 2000ee-3.

<sup>2</sup> 2015 DHS Data Mining Report available at:

<https://www.dhs.gov/sites/default/files/publications/2015%20Data%20Mining%20Report%20FINAL.pdf>.

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);<sup>4</sup> the E-Government Act of 2002 (E-Government Act);<sup>5</sup> 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 sustain[s], and do[es] not erode, privacy protections relating to the use, collection, and disclosure of personal information."<sup>6</sup>

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/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (December 29, 2008)<sup>7</sup> and in Department-wide directives including, most recently, Directive 047-01, Privacy Policy and Compliance (July 7, 2011).<sup>8</sup> 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), generally required by the E-Government Act,<sup>9</sup> and a System of Records Notice (SORN), generally required by the Privacy Act,<sup>10</sup> before the programs 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

---

<sup>3</sup> 6 U.S.C. § 121(d)(13).

<sup>4</sup> 5 U.S.C. § 552a.

<sup>5</sup> 44 U.S.C. § 3501 note.

<sup>6</sup> 6 U.S.C. § 142(a)(1).

<sup>7</sup> [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>8</sup> 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.

<sup>9</sup> 44 U.S.C. § 3501 note.

<sup>10</sup> 5 U.S.C. § 552a(e)(4).

compliance documentation is current, that personnel receive appropriate privacy training, and that privacy protections have been implemented.



## DHS PRIVACY OFFICE

### 2016 DATA MINING REPORT

### Table of Contents

EXECUTIVE SUMMARY .....	1
I. LEGISLATIVE LANGUAGE .....	7
II. DATA MINING AND THE DHS PRIVACY COMPLIANCE PROCESS .....	9
III. REPORTING .....	11
A. Automated Targeting System (ATS) .....	11
1. 2016 Program Update .....	11
a) Non-Immigrant and Immigrant Visa Applications .....	11
b) Overstay Vetting.....	12
c) Trusted Traveler Vetting.....	14
d) Electronic Visa Update System (EVUS).....	14
2. Special ATS Programs .....	15
a) Watchkeeper System.....	15
b) Secure Flight .....	16
c) Air Cargo Advance Screening Pilot.....	16
3. General ATS Program Description .....	16
a) ATS-Inbound (ATS-N) and ATS-Outbound (ATS-AT) Modules .....	19
b) ATS-Passenger (ATS-P) .....	22
c) ATS-Land Module (ATS-L) .....	25
4. ATS Privacy Impacts and Privacy Protections.....	27
B. Analytical Framework for Intelligence (AFI).....	30
1. 2016 Program Update .....	30
2. Program Description .....	30
3. Technology and Methodology .....	32
4. Data Sources .....	33

---

5.	Efficacy .....	35
6.	Laws and Regulations .....	35
7.	Privacy Impact and Privacy Protections.....	35
C.	FALCON Data Analysis and Research for Trade Transparency System (FALCON-DARTTS)..	38
1.	2016 Program Update .....	38
2.	Program Description .....	38
3.	Technology and Methodology .....	40
4.	Data Sources .....	42
5.	Efficacy .....	44
6.	Laws and Regulations .....	44
7.	Privacy Impact and Privacy Protections.....	45
D.	FALCON-Roadrunner .....	47
1.	2016 Program Update .....	47
2.	Program Description .....	48
3.	Technology and Methodology .....	49
4.	Data Sources .....	50
5.	Efficacy .....	52
6.	Laws and Regulations .....	52
7.	Privacy Impact and Privacy Protections.....	53
E.	DHS Data Framework.....	55
1.	2016 Program Update .....	55
2.	Program Description .....	57
3.	Technology and Methodology .....	58
4.	Data Sources .....	59
5.	Efficacy .....	60
6.	Laws and Regulations .....	60
7.	Privacy Impact and Privacy Protections.....	61
F.	SOCRATES Pilot .....	61
G.	Fraud Detection and National Security – Data System (FDNS-DS) .....	63
1.	Program Description .....	63
2.	Technology and Methodology .....	64
3.	Data Sources .....	66
4.	Efficacy .....	68
5.	Laws and Regulations .....	69
6.	Privacy Impact and Privacy Protections.....	69
IV.	CONCLUSIONS .....	71

---

V. APPENDIX ..... 72

---

## 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.<sup>11</sup>

The Act defines “data mining” as:

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

(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.<sup>12</sup>

<sup>11</sup> 42 U.S.C. § 2000ee-3(c).

<sup>12</sup> 42 U.S.C. § 2000ee-3(b)(1). “[T]elephone 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 or the Department) 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.<sup>13</sup> 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.<sup>14</sup> 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,<sup>15</sup> the E-Government Act of 2002,<sup>16</sup> 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 do[es] not erode, privacy protections relating to the use, collection, and disclosure of personal information.”<sup>17</sup>

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 of 1974. The FIPPs serve as DHS’s core privacy framework. They are memorialized in the Privacy Office’s Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security

---

<sup>13</sup> 6 U.S.C. § 142. The authorities and responsibilities of the Chief Privacy Officer were last amended by on August 3, 2007 by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53. 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 2016 Annual Report to Congress, available at: <https://www.dhs.gov/sites/default/files/publications/dhsprivacyoffice2016annualreport-FINAL-12122016.pdf>.

<sup>14</sup> The Act states that, “The responsibilities of the Secretary relating to intelligence and 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). This responsibility is carried out by the Under Secretary for Intelligence and Analysis pursuant to 6 U.S.C. § 121(c).

<sup>15</sup> 5 U.S.C. § 552a.

<sup>16</sup> 44 U.S.C. § 3501 note.

<sup>17</sup> 6 U.S.C. § 142(a)(1).

(December 29, 2008)<sup>18</sup> and in Department-wide directives including, most recently, Directive 047-01, Privacy Policy and Compliance (July 7, 2011).<sup>19</sup> The FIPPs govern the appropriate collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) at the Department in fulfillment 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);<sup>20</sup> (2) the Privacy Impact Assessment (PIA);<sup>21</sup> and (3) the System of Records Notice (SORN).<sup>22</sup> 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.<sup>23</sup> 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)<sup>24</sup> 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.

---

<sup>18</sup> [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>19</sup> Directive 047-01 and its accompanying Instruction are available at:

<https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf> and

<https://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-instruction-047-01-001.pdf>, respectively. The Directive supersedes the DHS Directive 0470.2, Privacy Act Compliance, which was issued in October 2005.

<sup>20</sup> The DHS privacy compliance process begins with a PTA, a required document that serves as the official determination by the DHS Privacy 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>.

<sup>21</sup> 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.

<sup>22</sup> 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).

<sup>23</sup> 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](http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s300.pdf).

<sup>24</sup> Title 44, U.S.C., Chapter 35, Subchapter II (Information Security).

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

### III. REPORTING

In the 2015 DHS Data Mining Report,<sup>25</sup> the DHS Privacy Office discussed the following Departmental programs that engage in data mining, as defined by the Act:

- The Automated Targeting System (ATS), which is administered by U.S. Customs and Border Protection (CBP) and includes modules for inbound (ATS-N) and outbound (ATS-AT) cargo, land border crossings (ATS-L), and passengers (ATS-P);
- The Analytical Framework for Intelligence (AFI), which is administered by CBP;
- The FALCON Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by U.S. Immigration and Customs Enforcement (ICE);
- The FALCON-Roadrunner system, which is administered by ICE; and
- The DHS Data Framework, which is a DHS-wide initiative.

This section of the 2016 report presents complete descriptions of these programs together with updates on modifications, additions, and other developments that have occurred in the current reporting year. In addition, this section provides descriptions of two additional Departmental programs that the DHS Privacy Office has determined engage in data mining:

- The SOCRATES Pilot Program, which is administered by CBP; and
- The Fraud Detection and National Security – Data System (FDNS-DS), which is administered by the United States Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security Directorate (FDNS).

#### A. Automated Targeting System (ATS)

##### 1. 2016 Program Update

###### a) Non-Immigrant and Immigrant Visa Applications

As described in the 2012 ATS PIA,<sup>26</sup> ATS-P (under the new User Interface of Unified Passenger) 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

<sup>25</sup> 2015 DHS Data Mining Report, *available at* <https://www.dhs.gov/sites/default/files/publications/2015%20Data%20Mining%20Report%20FINAL.pdf>.

<sup>26</sup> The ATS PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>.

vetting for non-immigrant visas. DoS sends online visa application data to ATS for pre-adjudication vetting. ATS vets the visa application and provides a response to the DoS's Consular Consolidated Database (CCD)<sup>27</sup> indicating whether DHS has identified derogatory information about the individual. Applications of individuals for whom derogatory information is identified through ATS are either vetted directly in ATS, if a disposition can be determined without further research, or additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net)<sup>28</sup> case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD. DoS plans to begin sending immigrant visa applications for vetting to CBP beginning in Fiscal Year (FY) 2017. 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-P 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<sup>29</sup> system for further investigation and possible enforcement action. In addition to prioritizing overstay leads, ATS is also used to vet overstay candidates received from the Arrival and Departure Information System (ADIS)<sup>30</sup> 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)<sup>31</sup>, Form I-94 Notice of Arrival/Departure records (derived from the Non-immigrant Information System (NIIS))<sup>32</sup>, and data from the DHS Student Exchange Visitor Information System (SEVIS).<sup>33</sup>

---

<sup>27</sup> The CCD PIA is available at: [https://foia.state.gov/\\_docs/pia/consularconsolidateddatabase\\_ccd.pdf](https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf).

<sup>28</sup> The VSPTS-Net PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>29</sup> 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 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>.

<sup>30</sup> 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>.

<sup>31</sup> The BCI PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>32</sup> The SORN for NIIS is available at: <https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05804.htm>.

<sup>33</sup> 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>.

As with the Phase 2 Pilot, discussed in DHS's 2013, 2014, and 2015 Data Mining Reports,<sup>34</sup> Phase 3 also uses foreign national overstay data obtained through system processing in ATS 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 (NPPD) to CBP.<sup>35</sup> 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 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,<sup>36</sup> the US-VISIT Technical Reconciliation Analysis Classification System,<sup>37</sup> and Overstay Vetting.<sup>38</sup>

In October 2015, the Overstay candidate's process was eliminated, and the weekly Overstay Leads process was moved to a daily process, streamlining the overall processing of Overstays. In May 2016, the data feed from the ICE SEVIS system was upgraded to a daily feed, to include additional data elements necessary for Overstay processing. CBP will work with ICE's Counterterrorism and Criminal Exploitation Unit to enhance the current interface with LeadTrac to include the additional data elements.

The legal authorities for the One DHS Overstay Vetting Pilot include: the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000, Public Law 106-215; the Visa Waiver Permanent Program Act of 2000, Public Law 106-396; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Public Law 107-56; EBSVERA; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53.<sup>39</sup>

---

<sup>34</sup> 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](http://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf). The 2015 Data Mining Report is available at:

<https://www.dhs.gov/sites/default/files/publications/2015%20Data%20Mining%20Report%20FINAL.pdf>.

<sup>35</sup> See Consolidated Appropriations Act, 2014, Pub. L. No. 113-76 (Jan. 17, 2014).

<sup>36</sup> The ATS PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>37</sup> See DHS/NPPD/USVISIT/PIA-004 available at: <http://www.dhs.gov/privacy-impact-assessments>. CBP will update the ATS and ADIS PIAs to reflect the move of ADIS from OBIM to CBP.

<sup>38</sup> 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. This PIA lists all of the SORNs applicable to this program and is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>39</sup> A complete list of authorities is included in the PIA for the Overstay Vetting Pilot, available at: <http://www.dhs.gov/privacy-impact-assessments>.

### c) Trusted Traveler Vetting

The vetting process for CBP's 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. All CBP Vetting Center officers completed the transition to vetting Trusted Travelers through ATS in February 2016. In October 2016, all targeting for new and updated applications was also fully transitioned to the ATS platform, as part of the TECS Modernization effort to interface with modernized Department of Justice's (DOJ) National Crime Information Center (NCIC) and Nlets queries.<sup>40</sup> 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. This capability was evaluated during a Pilot, and based on careful review of the applications that were marked for Auto-Conditional approval, CBP's Office of Field Operations authorized turning this capability on in March 2016.

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.

### d). Electronic Visa Update System (EVUS)

In October 2016, the vetting of Electronic Visa Update System (EVUS)<sup>41</sup> applications was enabled through ATS, in support of the launch of the public facing EVUS application. EVUS is the online system used by nationals of China holding a 10-year B1/B2, B1 or B2 (visitor) visa periodically to update basic biographic information to facilitate their travel to the United States. In addition to a valid visa, such travelers will be required to complete an EVUS enrollment to be

---

<sup>40</sup> TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC) Terrorist Screening Data Base (TSDB) and provides access to DOJ's NCIC, which contains information about individuals with outstanding wants and warrants, and to Nlets, a clearinghouse for state wants and warrants as well as information from state Departments of Motor Vehicles (DMV).

<sup>41</sup> See DHS/CBP/PIA-033 Electronic Visa Update System (EVUS) PIA available at: <http://www.dhs.gov/privacy-impact-assessments>.

admitted into the United States. DHS and DoS established EVUS under the authority granted in Immigration and Nationality Act (INA).<sup>42</sup> Section 221(a)(1)(B) of the INA authorizes the State Department to issue nonimmigrant visas to foreign nationals. Section 221(c) of the INA provides that “[a] nonimmigrant visa shall be valid for such periods as shall be by regulations prescribed,” and section 221(i) of the INA authorizes the Secretary of State to revoke visas at any time, in his or her discretion. Section 214(a)(1) of the INA specifically authorizes DHS to create conditions for an alien’s admission, and Section 215(a)(1) of the INA provides that aliens’ entry into the United States may be limited and conditioned by DHS. Section 103 of the INA and 8 CFR 2.1 authorize the Secretary of Homeland Security to administer and enforce the INA and other laws relating to the immigration and naturalization of aliens, and to establish such regulations as he deems necessary for carrying out his authority.

## 2. Special ATS Programs

### a) Watchkeeper System

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

USCG enhanced Watchkeeper by integrating the ATS-N and ATS-P 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.<sup>43</sup>

---

<sup>42</sup> INA sections 103 (8 U.S.C. §1103), 214 (8 U.S.C. § 1184), 215 (8 U.S.C. § 1185), 221 (8 U.S.C. § 1201), and 8 CFR Part 2.

<sup>43</sup> The PIA for Watchkeeper is available at: <http://www.dhs.gov/privacy-impact-assessments>.

## b) Secure Flight

TSA's Secure Flight Program (Secure Flight) continues to leverage real-time, threat-based intelligence rules run by ATS-P 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 on December 8, 2014.<sup>44</sup> An annex to this report containing Sensitive Security Information (SSI) about Secure Flight's use of ATS-P is being provided separately to the Congress. TSA's legal authorities related to passenger screening include: 49 U.S.C. § 114(d), (e), and (f), and 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, 2014, and 2015 Data Mining Reports,<sup>45</sup> using existing CBP data collections and ATS-N to identify pre-departure air cargo that may pose a threat to aviation security. In July 2016, CBP extended the pilot through July 26, 2017.<sup>46</sup> 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 also uses ATS to identify other potential violations of U.S. laws that CBP enforces at the border

---

<sup>44</sup> The Secure Flight PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>45</sup> 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](http://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf). The 2015 Data Mining Report is available at: <https://www.dhs.gov/sites/default/files/publications/2015%20Data%20Mining%20Report%20FINAL.pdf>.

<sup>46</sup> Extension of the Air Cargo Advance Screening (ACAS) Pilot Program and Reopening of Application Period for Participation, 81 Fed. Reg. 47812 (July 22, 2016), available at: <https://www.federalregister.gov/documents/2016/07/22/2016-17366/extension-of-the-air-cargo-advance-screening-acas-pilot-program>.

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,<sup>47</sup> 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-P (which involves analysis of information about certain travelers), and the ATS Targeting Framework (ATS-TF) (a platform for temporary and permanent storage of data).

The U.S. Customs Service, a legacy organization of CBP, traditionally employed computerized tools to target potentially high-risk cargo entering, exiting, and transiting the United States, 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<sup>48</sup> became operational in 1997. ATS-P (the new User Interface is now referred to as Unified Passenger, or UPAX)<sup>49</sup> became operational in 1999 and is now even more critical to CBP's mission. ATS-P allows CBP officers to determine whether a variety of potential risk indicators exist for travelers or their itineraries that may warrant additional scrutiny. ATS-P maintains Passenger Name Record (PNR) data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from certain air carriers in 1997. Currently, CBP collects this information to the extent it is collected by carriers in connection with a flight into or out of the United States, as part of CBP's border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).<sup>50</sup>

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

---

<sup>47</sup> At the time of this report, CBP maintains the export targeting functionality in 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.

<sup>48</sup> Functionality of ATS-AT was modernized when the AES system was recently re-engineered and deployed by CBP.

<sup>49</sup> UPAX is an updated user interface that replaced the older functionality of ATS-P.

<sup>50</sup> 49 U.S.C. § 44909. The regulations implementing ATSA are codified at 19 C.F.R. § 122.49d.

Information System (APIS), the Automated Commercial Environment (ACE), the Electronic System for Travel Authorization (ESTA), EVUS, Global Enrollment System (GES), the Nonimmigrant Information System (NIIS), BCI, the Seized Asset Case Tracking System (SEACATS), ICE's SEVIS and Enforcement Integrated Database (EID), and TECS.<sup>51</sup> TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)<sup>52</sup> TSDB and provides access to DOJ's NCIC, which contains information about individuals with outstanding wants and warrants, and to Nlets, a clearinghouse for state wants and warrants as well as information from state Departments of Motor Vehicles (DMV). ATS collects PNR data directly from air carriers. ATS also collects data from certain airlines, 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 the Automated Export System (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.

---

<sup>51</sup> PIAs for these programs can be found at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>52</sup> 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, available at <https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf>, 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.

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

### i. Program Description

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

The functionality of ATS-AT was modernized when the AES system was 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.<sup>53</sup> 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,<sup>54</sup> and other analytic techniques to enhance ATS-N and ATS-AT. This

---

<sup>53</sup> 6 U.S.C. §§ 901 *et seq.*

<sup>54</sup> 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

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 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,<sup>55</sup> 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) 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

---

automatically, using computational and statistical methods. This extracted information may then be generalized into rules and patterns.

<sup>55</sup> 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.

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.<sup>56</sup> 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 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, on March 20, 2016, CBP seized 123.85 kilograms of methamphetamine based on an NTC-C referral. NTC-C identified a shipment from Mexico to the United States as high risk for narcotic smuggling and referred the shipment to the appropriate port of entry for examination.

Additionally, on January 9, 2016, a CBP port of entry discovered 19.3 kilograms of opium based upon a referral from NTC due to a match to a narcotics rule.

---

<sup>56</sup> 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.

## 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.<sup>57</sup> ATS-AT and ATS-N also support functions mandated by Title VII, Counter-terrorism and Drug Law Enforcement, 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<sup>58</sup> and the 1996 Clinger-Cohen Act.<sup>59</sup> The risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.<sup>60</sup>

### b) ATS-Passenger (ATS-P)

#### i. Program Description

ATS-P is a custom-designed system used at U.S. ports of entry, particularly those receiving international flights and voyages (both commercial and private), and at the CBP NTC to evaluate passengers and crew members prior to their arrival to or departure from the United States. Unified Passenger (UPAX) is a technology refresh of ATS-P and was deployed as an update to the ATS-P functional interface in March 2013. ATS-P 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-P is a fully operational application that utilizes CBPs' System Engineering Life Cycle methodology<sup>61</sup> and is subject to recurring systems maintenance.

#### ii. Technology and Methodology

Unified Passenger (UPAX) is an updated user interface that replaces the older functionality of the ATS-P interface to process traveler information, as well as Visa, ESTA, EVUS, and GES 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 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

<sup>57</sup> 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.

<sup>58</sup> 22 U.S.C. §§ 5201 *et seq.*

<sup>59</sup> 40 U.S.C. §§ 1401 *et seq.*

<sup>60</sup> 6 U.S.C. § 912(b).

<sup>61</sup> 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.

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 or the applicant.

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

### iii. Data Sources

ATS-P uses available information from the following databases to assist in the development of the risk-based rules discussed above: APIS; NIIS, which contains all Form I-94 Notice of Arrival/Departure records and actual arrivals/departures; ESTA, which contains pre-arrival information for persons seeking authorization to travel under the Visa Waiver Program (VWP).<sup>62</sup>

---

<sup>62</sup> 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>.

GES, which contains trusted traveler application data; and the DoS visa databases. ATS-P also relies upon PNR information from air carriers, BCI crossing data, seizure data, Report of International Transportation of Currency or Monetary Instrument Report (CMIR) data,<sup>63</sup> and information from the TSDB and TECS.

#### iv. Efficacy

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

In the past year, ATS-P has identified, through lookouts and/or risk-based rule sets, individuals who were confirmed matches to the TSDB and caused action to be taken to subject them to further inspection or, in some cases, made recommendations to carriers not to board such persons. ATS-P matches have also enabled CBP officers and foreign law enforcement partners with whom CBP may share information to disrupt and apprehend persons engaged in human trafficking and drug smuggling operations. For example, CBP officers working at the NTC using ATS-P identified an individual with links to a terrorist involved in a terrorist attack. Based on the research conducted by the NTC, the subject was nominated to the TSDB, and based on the available information, DoS determined the individual was inadmissible and revoked the individual's visa. In another instance, CBP, working at the NTC in conjunction with the Internal Revenue Service (IRS) Criminal Investigation Division (CID), identified a Nigerian citizen with an active warrant for financial fraud and money laundering. Using ATS-P, CBP was able to provide information to IRS CID to assist in locating the fugitive, which subsequently led to his arrest.

#### v. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.<sup>64</sup> As part of this inspection and examination process, each traveler seeking to enter the United States must first establish his or her identity, nationality, and when appropriate, admissibility to the satisfaction of the CBP officer and then submit to inspection for customs purposes. The information collected is authorized pursuant to the EBSVERA,<sup>65</sup> ATSA,

<sup>63</sup> The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.

<sup>64</sup> 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.

<sup>65</sup> 8 U.S.C. § 1721.

IRTPA, the Immigration and Nationality Act (INA), and the Tariff Act of 1930, as amended.<sup>66</sup> 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), analytical correlation 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). Analytical correlation 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 correlation analysis to incoming vehicle and traveler data). The analytical correlation 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

---

<sup>66</sup> 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.

further official interest in a vehicle and its travelers or supporting information for the clearance and admission of the vehicle and its travelers.

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 travelers 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, Suspect and Violator Indices (SAVI)<sup>67</sup>, 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 May 2016, a CBP Officer assigned to a Port of Entry vehicle primary lane was inspecting the driver of a vehicle who declared nothing when attempting to enter the U.S. When the CBP Officer received an ATS-L alert, he referred the vehicle to secondary inspection. While in secondary, the CBP Officer obtained a second negative declaration from the driver, who stated that he was on his

---

<sup>67</sup> ATS-P maintains a copy of information from various systems, including SAVI, to identify individuals requiring additional screening prior to entering or exiting the country. The ATS PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>.

way home after a short stay in Mexico. During the inspection, a canine alerted the officer to the spare tire of the vehicle. CBP contacted agents from ICE Homeland Security Investigations (HSI), who removed the tire and found 50 packages, one of which tested positive on site for methamphetamine. In total, CBP and ICE HSI seized over 22 kilograms of methamphetamines. The ATS-L vehicle targeting capability directly facilitated this seizure, as checks on the driver raised no alerts. Without the ATS-L functionality, the driver might not have been sent to secondary inspection and as a result, the methamphetamines would not have been found.

#### v. Laws and Regulations

CBP is responsible for collecting and reviewing information about vehicles and their occupants prior to entering the United States.<sup>68</sup> 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-P (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 January 13, 2017,<sup>69</sup> and updated the SORN for ATS in May 2012. CBP, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties (CRCL), 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 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.<sup>70</sup> 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

<sup>68</sup> 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.

<sup>69</sup> ATS PIA Update is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>70</sup> 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.

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 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.<sup>71</sup>

In the event that PII (such as certain data within a PNR) used by or maintained in ATS-P is believed by the data subject to be inaccurate, the subject has access to the redress process previously developed by DHS. The data subject is provided information about this process during examination at secondary inspection. In addition, CBP officers have a brochure available to each individual entering and departing the United States that provides CBP's Pledge to Travelers. This pledge gives each traveler an opportunity to speak with a passenger service representative to answer any questions about CBP procedures, requirements, policies, or complaints.<sup>72</sup> 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,

---

<sup>71</sup> 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.

<sup>72</sup> 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.

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.<sup>73</sup>

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 additional means of access to PII held in source systems.<sup>74</sup> Privacy Act and FOIA requests for access to information for which ATS is the source system are directed to CBP.<sup>75</sup>

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 January 26, 2017, 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 October 28, 2025.

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.<sup>76</sup> The retention period for PNR, which is contained only in ATS-P, is subject to the following further access restrictions

---

<sup>73</sup> DHS TRIP can be accessed at: <http://www.dhs.gov/dhs-trip>.

<sup>74</sup> 5 U.S.C. § 552.

<sup>75</sup> Requests may be submitted by mail to FOIA Officer, 1300 Pennsylvania Avenue, NW, Room 3.3D, Washington, D.C. 20229 or electronically by visiting: <https://www.dhs.gov/freedom-information-act-foia>.

<sup>76</sup> NARA approved the record retention schedule for ATS on April 12, 2008.

and masking requirements: ATS-P 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.<sup>77</sup>

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

## B. Analytical Framework for Intelligence (AFI)

### 1. 2016 Program Update

AFI became the user interface for access to select datasets that formerly resided in ICE's Intelligence Fusion System (IFS) as discussed below in section III.B.4.<sup>78</sup>

On September 1, 2016, the AFI Privacy Impact Assessment was updated to include legacy IFS datasets that formerly resided in ICE's IFS, and to permit access to AFI by additional DHS components including United States Citizenship and Immigration Services (USCIS), United States Coast Guard, Transportation Security Administration, and DHS Office of Intelligence and Analysis (I&A).<sup>79</sup>

### 2. Program Description

CBP's AFI system provides enhanced search and analytical capabilities 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

<sup>77</sup> 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](http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf).

<sup>78</sup> 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>.

<sup>79</sup> The Updated PIA for AFI is available at: <http://www.dhs.gov/privacy-impact-assessments>.

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<sup>80</sup> 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 uses transaction-based systems such as TECS and ATS for targeting and inspections. AFI enhances the information from those systems by employing different analytical capabilities and tools that provide link analysis among data elements.

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. Finished intelligence products and unfinished "projects"<sup>81</sup> 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

---

<sup>80</sup> "Finished Intelligence Products" are intelligence reports or products developed through detailed analytic research from the collection, processing, integration, analysis, evaluation, and interpretation of available information, typically regarding long-term intelligence priorities.

<sup>81</sup> 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 Request for Information (RFI) response.

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, 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.<sup>82</sup>

### 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 regularly refresh data from the source system. 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.

---

<sup>82</sup> 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>.

- *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 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:
  - 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);
  - Select legacy IFS datasets (including the following information: EID 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).<sup>83</sup>
  - Enterprise Management Information System-Enterprise Data Warehouse (including: Arrival and Departure Form I-94<sup>84</sup>; CMIR<sup>85</sup> data; apprehension, inadmissibility, and seizure information from the ICE Criminal Arrest Records

<sup>83</sup> 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>.

<sup>84</sup> The PIA for DHS/CBP/PIA-024, Arrival and Departure Information System (ADIS) is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>85</sup> The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.

and Immigration Enforcement Records (CARIER);<sup>86</sup> National Security Entry-Exit Program information from CARIER; SEVIS<sup>87</sup> information; and seizure information from the Seized Asset and Case Tracking System<sup>88</sup>); and,

- The ATS-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.
- *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.<sup>89</sup>
- *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 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.

<sup>86</sup> The SORN for CARIER is available at: [https://www.regulations.gov/document?D=DHS\\_FRDOC\\_0001-1513](https://www.regulations.gov/document?D=DHS_FRDOC_0001-1513).

<sup>87</sup> 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>.

<sup>88</sup> The SORN for the Seized Assets and Case Tracking System is available at: <https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29802.htm>.

<sup>89</sup> 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>.

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, CBP received a request from the Drug Enforcement Administration (DEA) to help identify a passenger traveling from Central America to Italy suspected of importing cocaine. Using the AFI Matrix search with data criteria provided, CBP personnel were able to identify the traveler and provide enough travel history identifiers for DEA to locate, intercept, and arrest the traveler a few days later.

In another instance, all terminated students needed to be identified within a specific time frame from schools located in a specific area of responsibility. AFI's ability to retrieve information almost instantly allowed this request to be completed expeditiously. The student information was then run through the AFI batch search, which provided vital information needed in targeting individuals who could potentially cause risk to the United States.

## 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; 6 U.S.C. § 202 and 6 U.S.C. § 211.

## 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.<sup>90</sup> 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

---

<sup>90</sup> The PIA for AFI includes a more complete description of these protections and is available at: <http://www.dhs.gov/privacy-impact-assessments>.

opt-out of use information. AFI provides the public notice about its use of information through its PIA and SORN.<sup>91</sup>

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 PCRs for AFI on December 19, 2014<sup>92</sup> and December 6, 2016.<sup>93</sup>

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.<sup>94</sup> 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.

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

---

<sup>91</sup> 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>.

<sup>92</sup> The 2014 AFI PCR is available at: <http://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf>.

<sup>93</sup> The 2016 AFI PCR is available at: <https://www.dhs.gov/sites/default/files/publications/AFI%20PCR%20final%2012062016.pdf>.

<sup>94</sup> 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.

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 Sensitive But Unclassified (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 September 9, 2016, 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 Authorizations 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 exemptions 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.<sup>95</sup>

---

<sup>95</sup> Notwithstanding the applicable exemptions, CBP reviews all Privacy Act access requests 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 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>.

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, 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. 2016 Program Update

During the 2016 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.<sup>96</sup>

ICE published the PIA for FALCON-DARTTS on January 16, 2014<sup>97</sup> 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. The FALCON-SA PIA and Appendix have since been updated and republished for reasons unrelated to FALCON-DARTTS.<sup>98</sup> On December 1, 2014, ICE republished the Trade Transparency Analysis and Research (TTAR) SORN, which applies to FALCON-DARTTS.<sup>99</sup>

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

---

<sup>96</sup> 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-032(a) FALCON Search & Analysis System (FALCON-SA), January 16, 2014, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>97</sup> See DHS/ICE/PIA-038 FALCON-DARTTS, January 16, 2014, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>98</sup> See DHS/ICE/PIA-032(b) FALCON-SA, October 11, 2016, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>99</sup> 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 was 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.<sup>100</sup> 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 predetermined 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.

---

<sup>100</sup> 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.

Specifically, only ICE HSI and CBP users are granted access to the law enforcement data, and only ICE HSI users are granted access to the financial data, maintained in FALCON's general data storage environment.<sup>101</sup> 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,<sup>102</sup> link analysis, and charting and graphing tools that use proprietary statistical algorithms.<sup>103</sup> 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.

---

<sup>101</sup> 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.

<sup>102</sup> 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.

<sup>103</sup> 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.

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

FALCON-DARTTS also performs financial data analysis by analyzing financial reporting data (the import and export of currency, deposits of currency in financial institutions, reports of suspicious financial activities, and the identities of parties to these transactions) to identify patterns of activity that may indicate money laundering schemes.

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

FALCON-DARTTS uses trade data, financial data, and law enforcement data provided by other U.S. government agencies and foreign governments (hereafter referred to as “raw data”).<sup>104</sup> 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.<sup>105</sup> 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.<sup>106</sup> 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

---

<sup>104</sup> 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.

<sup>105</sup> 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.

<sup>106</sup> 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.

abroad use the analyses to respond to inquiries from foreign partner TTUs. If a foreign TTU identifies suspicious U.S. trade transactions of interest, HSI investigators will validate that the transactions are, in fact, suspicious, and ICE will coordinate joint investigations on those specific trade records. ICE may also open its own investigation into the matter.

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

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

## 4. Data Sources

All raw data analyzed by FALCON-DARTTS is provided by other U.S. agencies and foreign governments, and is divided into the following broad categories: U.S. trade data, foreign trade data, financial data, and law enforcement data. U.S. trade data is (1) import data in the form of an extract from ACS, which CBP collects from individuals and entities importing merchandise into the United States who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via ACS; (2) EEI submitted to AES; and (3) bill of lading data collected by 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 the Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) or federal, state, and local law enforcement agencies. Bank Secrecy Act (BSA) data is in the form of the following financial transaction reports: Currency and Monetary Instrument 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,<sup>107</sup> 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.<sup>108</sup>

ICE receives law enforcement records from the Specially Designated Nationals (SDN) List<sup>109</sup> 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

---

<sup>107</sup> 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.

<sup>108</sup> 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.

<sup>109</sup> As part of its enforcement efforts, the Department of Treasury's Office of Foreign Assets Control (OFAC) publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.

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 in 2016. For example, special agents with HSI El Paso used FALCON-DARTTS in a money laundering [18 U.S.C. § 1956(h)] investigation involving the owner of a sports store. In January 2016, the owner was convicted and sentenced to 121 months in Federal prison for implementing an estimated \$100 million trade-based money laundering scheme. By pleading guilty, the owner admitted he and others conspired to launder the proceeds of a scheme to illegally smuggle goods into Mexico without paying the tariffs, duties, and fees imposed by the Mexican government. From March 6, 2006, to November 2014, these goods were ultimately smuggled using “pasadores,” or black market smugglers, without following U.S. laws and regulations regarding the export of goods from the United States. Evidence presented during trial also revealed that, between 2012 and 2014, more than an estimated \$2.3 million in bribes were paid to Mexican customs officials to facilitate the scheme. 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.

## 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,<sup>110</sup> the Trade Secrets Act,<sup>111</sup> and the BSA.<sup>112</sup>

## 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.<sup>113</sup> FALCON-DARTTS will coordinate requests for access or to amend data with the original data owner. ICE published a PIA for FALCON-DARTTS on January 16, 2014, and republished the SORN that applies to FALCON-DARTTS on December 1, 2014.<sup>114</sup>

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

---

<sup>110</sup> 5 U.S.C. § 552a.

<sup>111</sup> 18 U.S.C. § 1905.

<sup>112</sup> 31 U.S.C. § 5311.

<sup>113</sup> 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) available at: <https://www.gpo.gov/fdsys/pkg/FR-2014-04-14/pdf/2014-08254.pdf>, and for CBP Information, Import Information System (DHS/CBP-001) available at: <https://www.regulations.gov/document?D=DHS-2016-0048-0001> and TECS (DHS/CBP-011) available at: <http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm>.

<sup>114</sup> FALCON-DARTTS is covered by the SORN for the ICE Trade Transparency and Analysis Research (TTAR) system of records available at: <http://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm>.

information pertains.<sup>115</sup> 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 identify users who are using the system improperly.<sup>116</sup>

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

---

<sup>115</sup> 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.

<sup>116</sup> For more information on these controls, auditing, and accountability, see the FALCON-SA PIA available at: <http://www.dhs.gov/privacy-impact-assessments>.

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. Until the proposed retention schedule is approved, FALCON-DARTTS will continue to use the legacy DARTTS retention schedule. In the proposed retention schedule, case data generated by FALCON-DARTTS will be retained for ten years. Some of the data accessed 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 (e.g., trade data) 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. 2016 Program Update

During the 2016 reporting period, 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.<sup>117</sup>

ICE published the FALCON-Roadrunner PIA on November 12, 2014.<sup>118</sup> On December 1, 2014, ICE republished the TTAR SORN to expand its coverage to FALCON-Roadrunner.<sup>119</sup> Lastly, ICE updated the FALCON-SA PIA Appendix to capture the immigration, law enforcement, and

---

<sup>117</sup> 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>.

<sup>118</sup> FALCON-Roadrunner PIA available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>119</sup> See DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) SORN available at: <https://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm>.

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.

## 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;<sup>120</sup> weapons of mass destruction; or chemical, biological, radiological, and nuclear materials. The HSI Counter-Proliferation Investigations (CPI) Program oversees a broad range of investigative activities related to such violations of law. The CPI Program enforces U.S. laws governing the export of military items, controlled dual-use goods, firearms, and ammunition, as well as exports to sanctioned or embargoed countries.

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

- *Investigative Lead Generation:* FALCON-Roadrunner allows CPI investigators and analysts to generate leads for, and otherwise support, investigations of export violations within the jurisdiction of HSI. By using FALCON-Roadrunner to analyze trade data, CPI investigators and analysts are able to identify anomalous transactions and activities that may be indicative of export violations and warrant investigation. Experienced HSI investigators independently confirm and further investigate these anomalies.
- *Statistical/Trend Analysis:* FALCON-Roadrunner provides export enforcement-related statistical reporting capabilities, derived from trade data that investigators access. Statistical analytics and trend analysis is provided to the Export Enforcement Coordination Center, which is the primary forum within the Federal Government for executive departments and agencies to coordinate and enhance their export control enforcement activities.

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

---

<sup>120</sup> 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.

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<sup>121</sup> 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.

---

<sup>121</sup> With 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<sup>122</sup> 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<sup>123</sup> and the publicly available consolidated U.S. export screening lists of the U.S. Department of Commerce, State, and Treasury.<sup>124</sup> 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.<sup>125</sup>

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.<sup>126</sup>

---

<sup>122</sup> 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>.

<sup>123</sup> 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](http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm).

<sup>124</sup> *See* [www.export.gov/ecr/eg\\_main\\_023148.asp](http://www.export.gov/ecr/eg_main_023148.asp).

<sup>125</sup> 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.

<sup>126</sup> *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*

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.<sup>127</sup>

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

During the 2016 reporting period the integrated FALCON-Roadrunner program completed 133 support requests, furthering 37 active criminal investigations. FALCON-Roadrunner data analysis assisted HSI criminal investigators in 7 criminal arrests, 16 indictments, 6 convictions, and 5 administrative arrests. FALCON-Roadrunner analysis also assisted in the seizure of arms, ammunition, currency, vehicles, and computers with a monetary value of \$336,722 as well as 26.61 pounds of narcotics. FALCON-Roadrunner also produced in depth reports addressing the dumping of aluminum tubing produced in China on the U.S. market, transducers used in nuclear refinement, high risk nuclear commodities at risk of diversion, space and missile technology exports, oil drilling equipment destined for high risk geographic areas, U.S arms and ammunition exports, exports at risk of trans-shipment to North Korea, analysis of the new 600 series export control classification numbers, and additive manufacturing.

## 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

---

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>.

<sup>127</sup> 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>.

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.

## 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, but may be denied if 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.<sup>128</sup> 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.<sup>129</sup>

<sup>128</sup> 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: Import Information System (DHS/CBP-001) available at: <https://www.regulations.gov/document?D=DHS-2016-0048-0001>. DHS/CBP-011 TECS SORN 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 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 at: <https://www.gpo.gov/fdsys/pkg/FR-2010-03-01/html/2010-4102.htm>; and DHS/ICE-012 Visa Security Program Records SORN available at: at <http://www.gpo.gov/fdsys/pkg/FR-2009-09-30/html/E9-23522.htm>.

<sup>129</sup> FALCON-Roadrunner is covered by the following SORN: DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) available at: <https://www.gpo.gov/fdsys/pkg/FR-2014-12-01/html/2014-28168.htm>.

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

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

Any violations of FALCON-Roadrunner 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.<sup>130</sup>

ICE intends to request NARA approval on the following proposed ICE records schedule: The data generated by the system will be retained 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.

---

<sup>130</sup> FALCON-SA PIA available at: <http://www.dhs.gov/privacy-impact-assessments>.

## E. DHS Data Framework

### 1. 2016 Program Update

DHS continues to mature its Department-wide big data program, the DHS Data Framework.<sup>131</sup> In 2016, the Framework continued its Initial Operational Capability Phase. The current iteration of the Framework includes Neptune,<sup>132</sup> an unclassified platform, and Cerberus,<sup>133</sup> 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 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.<sup>134</sup>
- **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.<sup>135</sup>
- **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 introduce 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.<sup>136</sup>

In 2016, DHS focused on adding additional data sets, improving data quality and usability, supporting DHS sharing with the Intelligence Community, and developing a governance process to approve the use of analytical tools on Data Framework data.

As of October 11, 2016, seventeen data sets have been approved for inclusion in the Initial Operational Capability. These data sets are identified in sub-section 4 below.

---

<sup>131</sup> PIAs for the DHS Data Framework are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>132</sup> Neptune PIAs are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>133</sup> Cerberus PIAs are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>134</sup> For more information about the Pilot phase, please see the following PIAs: DHS/ALL/PIA-046 DHS Data Framework (November 2013); 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>.

<sup>135</sup> For more information about the Limited Production Capability phase, please see the following PIAs: DHS/ALL/PIA-046(a) DHS Data Framework; 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>.

<sup>136</sup> For more information about the Initial Operational Capability Phase, please see the DHS/ALL/PIA-046 DHS Data Framework, available at: <http://www.dhs.gov/privacy-impact-assessments>.

Initially, the Framework planned to enforce source IT system data requirements, including retention, in the Framework by relying on the source IT systems to notify the Framework of changes, deletions, or corrections to data. Therefore, DHS would not delete any data until the Framework received a delete notification from the source IT system. However, through the coordination of data delivery with dataset owners, the Department discovered that the source IT systems are not always able to accommodate this request due to a number of constraints, such as resources, legacy systems, and disruptions to operational support.

While the Department continues to prefer that the source IT systems provide deletion notifications to the Framework as described in previous DHS Data Framework PIAs, this solution is not always practicable at this point in time given the constraints described above. To address this issue, DHS has developed and deployed a data management capability within the Framework that manages the source IT system retention rules internally based on direction from the source IT system to ensure that the Framework continues to follow the source IT system's retention rules. This change to Data Framework's management of retention will be detailed in a forthcoming PIA.

During the Initial Operational Capability Phase, DHS will expand the DHS users of the Data Framework. In 2016, the Data Framework added new DHS users, but users of the Data Framework's Cerberus system remained limited to the counterterrorism purpose.

One of the most significant developments in 2016 is that DHS began using Cerberus to facilitate "bulk information sharing"<sup>137</sup> with U.S. Government partners.<sup>138</sup> As part of this sharing, Neptune provides Cerberus with certain Data Framework data that Cerberus shares externally, but Neptune itself does not share any information external to DHS. Cerberus provides the technical architecture to reduce or replace existing external information sharing mechanism among U.S. Government partners. Additionally, Cerberus allows DHS to share information through secure, automated connections rather than through ad hoc transfers of portable media (e.g., discs or hard drives). Any external sharing activities that use the Cerberus architecture must be described in the appropriate PIA for those projects and covered by a routine use in the SORN for the source DHS IT system. Additionally, all external sharing through Cerberus must be governed by an Information Sharing and Access Agreement (ISAA), such as a Memorandum of Agreement (MOA).

---

<sup>137</sup> Bulk information sharing is not linked to a particular number of records. Instead, bulk information sharing is determined by whether the information shared is sufficiently tailored to reasonably exclude information that is not relevant to a partner's request for data. Bulk information sharing refers to the transmission of large quantities of intelligence or information, which, due to technical or operational considerations, is transmitted without the use of discriminants reasonably likely to exclude any intelligence or information not relevant to the need giving rise to the recipient's request (specific identifiers, selection terms, etc.). For example, transmitting a list of known or suspected terrorists in response to a request for such information would not constitute a bulk data transfer because the request and its response are limited in scope to information reasonably likely to be of value to the recipient, but transmitting information about a group of individuals for the purpose of identifying known or suspected terrorists within that group would qualify as a bulk data transfer.

<sup>138</sup> DHS/ALL/PIA/046(c) DHS Data Framework – External Sharing (March 30, 2016), *available at* <http://www.dhs.gov/privacy-impact-assessments>.

In 2015, DHS created an interim data transfer process to address an emergent threat.<sup>139</sup> This interim process foregoes some of the automated protections of the Framework, such as the enforcement of access control policies in the classified data lake, to expedite its ability to meet a critical mission need. This interim data transfer process supported DHS's 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 interim solution will only continue until the standard model is capable of meeting the mission need. In 2016, DHS continued its preparations to end the interim data transfer solution as the Data Framework enhances its capabilities. DHS met with users of the interim solution and defined a set of operational requirements that the Data Framework must meet in order to fully replace the interim process. DHS made significant progress on meeting these requirements in 2016. 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 of 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

---

<sup>139</sup> DHS/ALL/PIA-051 DHS Data Framework – Interim Process to Address an Emergent Threat (April 15, 2015), available at <http://www.dhs.gov/privacy-impact-assessments>.

and civil liberties, and other legal and policy protections, and 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.<sup>140</sup> Currently, accessing relevant information 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 Framework 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.

---

<sup>140</sup> 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.

## 4. Data Sources

As of October 11, 2016, seventeen data sets have been approved for inclusion in the Initial Operational Capability. These data sets are listed in Appendix A<sup>141</sup> of the Framework PIA and include:

- Electronic System for Travel Authorization (ESTA);<sup>142</sup>
- Alien Flight Student Program (AFSP);<sup>143</sup>
- Student Exchange Visitor Information System (SEVIS);<sup>144</sup>
- Advance Passenger Information System (APIS);<sup>145</sup>
- Form I-94;<sup>146</sup>
- Passenger Name Record (PNR);<sup>147</sup>
- Section 1367 Data Extracted from the Central Index System;<sup>148</sup>
- Refugee, Asylum, and Parole System (RAPS);<sup>149</sup>
- Ship Arrival Notification System (SANS);<sup>150</sup>
- Border Crossing Information (BCI);<sup>151</sup>
- Automated Biometric Identification System (IDENT) Asylum Data;<sup>152</sup>
- Aviation Worker Data<sup>153</sup>;
- Airspace Waivers and Flight Authorizations for Certain Aviation Operations (including DCA) Data;<sup>154</sup>

<sup>141</sup> 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>.

<sup>142</sup> DHS/CBP/PIA-007 Electronic System for Travel Authorization available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>143</sup> DHS/TSA/PIA-026 Alien Flight Student Program (AFSP) available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>144</sup> DHS/ICE/PIA-001 Student Exchange Visitor Information System (SEVIS) available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>145</sup> DHS/CBP/PIA-001 Advance Passenger Information System (APIS) available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>146</sup> DHS/CBP/PIA-016 for Form I-94 Automation is available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>147</sup> 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>.

<sup>148</sup> 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>.

<sup>149</sup> DHS/USCIS/PIA-27 Refugee, Asylum and Parole System and the Asylum Pre-Screening System available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>150</sup> DHS/USCG/PIA-006(b) Vessel Requirements for the Notice of Arrival and Departure (NOAD) and Automatic Identification System (AIS) Rulemaking available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>151</sup> DHS/CBP/PIA-004(g) Beyond the Border Entry/Exit Program Phase II available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>152</sup> DHS/USCIS/PIA-27 Refugee, Asylum and Parole System and the Asylum Pre-Screening System available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>153</sup> DHS/TSA/PIA-020, Security Threat Assessment for Airport Badge and Credential Holders (SIDA) available at: <http://www.dhs.gov/privacy-impact-assessments>.

- Maryland-Three (MD-3) Airports Data;<sup>155</sup>
- Private Charter and Twelve Five Program Data,<sup>156</sup>
- Secure Flight Confirmed Matches Data;<sup>157</sup> and
- Bill of Lading.<sup>158</sup>

DHS will update Appendix A of the Framework PIA as new data sets are added. 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 Phase to the Initial Operational Capability Phase for both the Neptune and Cerberus systems. During the Initial Operational Capability Phase, DHS will add new DHS data sets and new users from DHS. DHS will provide additional information in future Data Mining Reports on the efficacy of the Framework.

## 6. Laws and Regulations

The DHS Data Framework is authorized by 6 U.S.C. § 121(d)(13), which directs the Secretary, through the Under Secretary for Intelligence and Analysis, to, among other things, “establish and utilize, in conjunction with the [C]hief [I]nformation [O]fficer 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”; 40 U.S.C. § 11315(b)(2), which provides that “[t]he Chief Information Officer of an executive agency is responsible for,” among other things, “developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for the executive agency”; and 44 U.S.C. § 3506 (a)(2), (b)(1)(C), which requires the head of each executive agency to designate a Chief Information Officer, who shall, among other things, “improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy and security.”

<sup>154</sup> DHS/TSA/PIA-020 Security Threat Assessment for Airport Badge and Credential Holders (SIDA) available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>155</sup> DHS/TSA/PIA-022 Maryland Three (MD-3) Airports available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>156</sup> DHS/TSA/PIA-017 Large Aircraft Security Program available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>157</sup> DHS/TSA/PIA-018(g) Secure Flight Program available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>158</sup> DHS/CBP/PIA-003(b) Automated Commercial Environment (ACE) available at: <https://www.dhs.gov/privacy-impact-assessments>.

## 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,<sup>159</sup> Cerberus,<sup>160</sup> Neptune,<sup>161</sup> Common Entity Index (CEI),<sup>162</sup> and the Interim Process to Address an Emergent Threat.<sup>163</sup> 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.<sup>164</sup>

### F. SOCRATES Pilot

CBP's Commercial Targeting and Enforcement Directorate (CTE), within the Office of International Trade (OT), is currently working on a project with the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to provide commercial trade data to enhance and identify pattern identification, entity links, and anomalies within large datasets. As part of CBP's mission, OT identifies trade risks that may include transshipment schemes to evade the payment of Anti-dumping and Countervailing duties (AD/CVD),<sup>165</sup> the filing of false Free Trade Agreement claims, and the use of identity theft to facilitate the importation of counterfeit merchandise. This project was initiated to determine the analytical abilities JHU/APL could apply to trade data analytics. During Fiscal Year (FY) 2016, a pilot test was completed by JHU/APL using import data.

<sup>159</sup> DHS/ALL/PIA-046 DHS Data Framework. Multiple iterations are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>160</sup> DHS/ALL/PIA-046-3 Cerberus. Multiple iterations are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>161</sup> DHS/ALL/PIA-046-1 Neptune. Multiple iterations are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>162</sup> DHS/ALL/PIA-046-2 Common Entity Index Prototype. Multiple iterations are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>163</sup> DHS/ALL/PIA-051 DHS Data Framework – Interim Process to Address an Emergent Threat, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>164</sup> 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 Prototype. Multiple iterations are available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>165</sup> AD/CVD are additional duties determined by the U.S. Department of Commerce, which offset unfair low prices and foreign government subsidies on certain imported goods. CBP enforces approximately 300 AD/CVD orders on over 150 commodities.

JHU/APL uses a government-off-the-shelf product named SOCRATES, developed by mathematicians at JHU/APL. SOCRATES, in conjunction with supporting software, is used to develop algorithms to analyze large datasets looking for both normal and abnormal trade patterns of behavior. This results in the identification of anomalies in trade patterns or behaviors that may indicate illicit or criminal behavior in the trade environment. An anomaly may also indicate behavior that is completely within the law and is legal; though, it may not fit within the normal trade behavior of the dataset. These anomalies lead to the examination of real time importations, matching against the anomalies, to determine if a violation of law or illicit activity occurred. Initial test results performed on import data provided positive results of trade anomalies that will be validated for illicit trade activity during the next test phase in FY2017.

The pilot data utilized by SOCRATES was obtained from the OT Analytical Development Division (ADD) Warehouse, the main data repository for OT, which also contains CBP historical data. The data in the ADD Warehouse is extracted from ATS<sup>166</sup> and ACE<sup>167</sup> on a monthly basis. The data being pulled from ATS consists only of cargo examination data contained in the Cargo Enforcement Reporting and Tracking System (CERTS) portion of ATS. ACE data includes entry summary transactions filed with CBP by importers for the last 10 years of transaction data. This data contains information such as importer numbers, as well as the trade data elements contained within the required commercial entry documents (e.g., Bill of Lading, Entry, and Entry Summary).<sup>168</sup> SOCRATES does not interact directly with CBP's systems, but is housed on CBP servers connected to CBP's network. Only CBP-cleared JHU/APL team members who have signed a non-disclosure agreement, have a CBP Personal Identity Verification card, and CBP network access can work on SOCRATES and CBP Trade Data. User activity is logged by the CBP Office of Information Technology (OIT) and by the CBP server housing SOCRATES. OIT will be implementing additional security measures, such as the capability to track more detailed user activity, in future enhancements.

The project is in the process of completing its testing phase and will proceed to validate the results during FY 2017. Validation of the results include CBP analysts or subject matter experts reviewing and determining whether the analytic results compare to past CBP findings, or provide additional recommendations for further review. Additional review of the analytics selections and in-depth determinations would be conducted for results outside of past CBP findings. Decisions about individuals or entities, normally referred to as Importers of Record, may be made during the validation phase in order to test the results of analytics as they are developed; any decisions would involve requests for examination or document review.

---

<sup>166</sup> ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments.

<sup>167</sup> ACE is a commercial trade processing system designed to automate border processing, enhance border security, and foster U.S. economic security through lawful international trade and travel.

<sup>168</sup> The "Entry" is filed when cargo reaches a port of entry, and provides the required information for CBP to make cargo release decisions, while the "Entry Summary" is filed within 10 business days of release and provides information for CBP to make duty and statistical calculations, and ensure that other requirements of law have been met.

The legal authorities for CBP's SOCRATES pilot include: 6 U.S.C. § 115(a)(1) and § 212(b)(2), 19 U.S.C. Chapter 4, 19 U.S.C. § 1592, 31 U.S.C. § 3729, 19 U.S.C. § 1481-1529, 19 U.S.C. § 1641, 31 U.S.C. § 7701(c), 19 CFR Part 24, and 19 CFR Part 149.3.

CBP is reviewing the compliance documentation for the use of SOCRATES as the reporting period for this report ended. In future Data Mining Reports, CBP will provide additional information on SOCRATES as it becomes operational.

## G. Fraud Detection and National Security – Data System (FDNS-DS)

### 1. Program Description

Every year, USCIS receives nearly 6.4 million applications for immigration benefits or service requests. USCIS is committed to ensuring the integrity of the U.S. immigration system. An integral part of USCIS's delegated authority to adjudicate benefits, petitions, or requests, and to determine if individuals are eligible for benefit or services, is to conduct screenings (i.e., background, identity, and security checks) on forms filed with the agency. USCIS/FDNS developed the Fraud Detection and National Security – Data System (FDNS-DS)<sup>169</sup> to record, track, and manage the screening processes related to immigration applications, petitions, or requests with suspected or confirmed fraud, public safety, or national security concerns. FDNS also uses FDNS-DS to identify vulnerabilities that may compromise the integrity of the legal immigration system.

Traditionally, FDNS-DS performed case management and received information primarily through manual referrals of cases from USCIS adjudications staff to FDNS Officers. In 2014, FDNS further enhanced FDNS-DS with a screening module known as ATLAS to automate the screening and matching of biometric and biographic information against databases containing arrest records or documented national security or public safety concerns. Through ATLAS, information is screened through a predefined set of rules to determine whether the information provided by the individual or obtained through the required background, identity, and security checks presents a potential fraud, public safety, or national security concern. ATLAS produces system generated notifications (SGN) that automate the process of referring cases for FDNS Officers' manual review.

ATLAS's screening capability enhances the integrity of the immigration process and strengthens USCIS's obligations of the Immigration and Nationality Act (INA) through the following benefits:

---

<sup>169</sup> The FDNS-DS PIA is available at: <http://www.dhs.gov/privacy-impact-assessments>. The FDNS SORN is available at: <https://www.gpo.gov/fdsys/pkg/FR-2012-08-08/html/2012-19337.htm>.

- Reduces application cycle time by creating SGNs to preemptively notify FDNS Officers of suspected fraudulent or nefarious information before adjudicators begin reviewing application;
- Increases consistency and timeliness for background and security check operations;
- Employs analytical tools to view non-obvious relationships across data and to detect fraudulent patterns in immigration benefit requests and applications;
- Ensures consistent process and procedures to operationalize screening enhancements; and,
- Integrates screening capabilities with USCIS case management systems.

FDNS is continuing to enhance its screening processes by incorporating seven core capabilities into ATLAS: (1) Predictive Analytics; (2) Link and Forensic Analysis; (3) Unstructured and Structured Analytics; (4) Intelligent Investigative Case Management; (5) Operational Decision Management; (6) Information Sharing and Collaboration; and (7) Entity Analytics.

## 2. Technology and Methodology

ATLAS is an enhanced screening platform that augments existing checks performed on immigration filings made to USCIS. The types of checks performed on immigration forms vary by the benefit/request type. In general, USCIS conducts background checks to obtain relevant information in order to render the appropriate adjudicative decision with respect to the benefit or service sought, identity checks to confirm the individual's identity and combat potential fraud, and security checks to identify potential threats to public safety or national security. Standard checks may include: biometric, fingerprint-based checks such as the FBI Fingerprint Check; DHS's IDENT Fingerprint Check<sup>170</sup>; and Department of Defense Automated Biometric Identification System (ABIS) Fingerprint Check<sup>171</sup>; and biographic, name-based checks such as the FBI Name Check; and TECS<sup>172</sup> Name Check.

USCIS uses several systems to support the requisite background, identity, and security checks, which are described in detail in various USCIS PIAs. As mentioned in those PIAs, USCIS adjudications staff must query multiple systems, in some cases manually. Through the development of ATLAS, the need to independently query each system is greatly reduced, thereby streamlining the screening process and limiting the privacy risks associated with using multiple systems. ATLAS interfaces with other systems in order to automate system checks and

<sup>170</sup> See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>171</sup> For certain benefit types in which the beneficiary has a higher likelihood of having previously been fingerprinted by the U.S. military, USCIS conducts checks against the Department of Defense's Automated Biometric Identification System, as described in the Customer Profile Management Service (CPMS) PIA. See DHS/USCIS/PIA-060 CPMS, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>172</sup> See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), available at: <http://www.dhs.gov/privacy-impact-assessments>.

promotes consistent storage, retrieval, and analysis of screening results to enable FDNS to detect and investigate fraud, public safety, and national security concerns more timely and effectively.

Within FDNS-DS, ATLAS's automated, event-based screening is triggered when:

1. An individual presents him or herself to the agency (e.g., when USCIS receives an individual's benefit request form or while capturing an individual's 10-fingerprints at an authorized biometric capture site, for those forms that require fingerprint checks);
2. Derogatory information is associated with the individual in one or more DHS systems; or
3. FDNS performs an administrative investigation.

ATLAS receives information from the individual's form submission and from the biographic and biometric-based checks listed above. That information is screened through a predefined set of rules to determine whether the information provided by the individual or obtained through the required checks presents a potential fraud, public safety, or national security concern. The rules help standardize how information is analyzed and help to detect patterns, trends, and risks that are not easily apparent from the form submissions themselves.

Screening through ATLAS automates the process of referring cases to FDNS for review. Certain events, such as when USCIS receives a benefit request form or the 10-print capture of an individual's fingerprints at a biometric capture center, trigger rules-based screening. If the benefit request form or biometric capture matches a rule, ATLAS produces an SGN, which is elevated in FDNS-DS for manual review. Once an SGN is produced, a specially trained FDNS Officer, known as a Gatekeeper, conducts a manual review of the SGN for validity, determines whether it is "actionable" or "inactionable," and, if "actionable," triages the SGN for further action. If an SGN is "actionable," it enters the formal FDNS-DS case management process. An SGN found to be "inactionable" may be closed without further action. The SGN itself is not considered derogatory. SGNs help FDNS Officers to detect potential threats earlier in the immigration benefit application process, to demonstrate the fidelity of the individual's biographic and biometric information, and to identify discrepancies more efficiently.

If FDNS determines an administrative investigation is necessary, FDNS conducts further checks to verify information prior to an adjudicative decision on the immigration benefit or service requested, to include resolving any potential fraud, public safety, or national security concerns. FDNS may perform administrative investigations or work with partner agencies, as appropriate, and ultimately produces findings to sufficiently inform adjudications.

ATLAS's analytical capabilities enable its users to more easily query and visualize data within the system and to identify individuals who are filing for immigration and naturalization benefits who may potentially be engaging in fraudulent behavior or pose a risk to public safety or national security. During the screening process, ATLAS analyzes the results of biographic and biometric checks, applies rules, and performs link and forensic analysis and entity resolution among data received from multiple systems. ATLAS assists in confirming individuals' identities

when individuals are potentially known by more than one identity by comparing the identity information provided by the individual with identity information in other systems checked against the background, identity, and security check process. As an example, ATLAS can determine if an individual has applied for benefits using multiple biographic identities or aliases. ATLAS also visually displays linkages or relationships among individuals to assist in identifying non-obvious relationships among individuals and organizations with a potential nexus to criminal or terrorist activities. The results of this analysis may be produced and elevated in FDNS-DS in the form of an SGN. Additionally, ATLAS comprises an advanced search functionality that allows FDNS-DS users to view the entire screening history on an individual, including records of standard checks, any SGNs produced by ATLAS that relate to the individual, and administrative investigations performed.

ATLAS's analytical capabilities do not alter the source data. All legal and policy controls around the source data remain in place.

### 3. Data Sources

The type of information collected depends on the specific context of a given case within FDNS-DS. Below is a list of systems, both internal and external, that exchange data with FDNS-DS, including those used to support screening through ATLAS.

*U.S. Citizenship and Immigration Services (USCIS) Systems:* National Benefit Center Process Workflow Repository (NPWR)<sup>173</sup> to facilitate screening on certain form types being processed through the National Benefit Center, Background Check Unit; Service Center Computer Linked Application Information Management System (SCCLAIMS)<sup>174</sup> to facilitate screening on forms processed in Computer Linked Application Information Management System (CLAIMS 3)<sup>175</sup>; CLAIMS 4<sup>176</sup>; Electronic Immigration System (ELIS)<sup>177</sup>; Case and Activity Management for International Operations (CAMINO)<sup>178</sup>; Refugees, Asylum, and Parole System and the Asylum Pre-Screening System (RAPS/APSS)<sup>179</sup>; Marriage Fraud Assurance System (MFAS); Adoption Case Management System (ACMS); USCIS Lockbox<sup>180</sup> to retrieve data from digitized forms; Person Centric Query Service (PCQS)<sup>181</sup> to retrieve status information from the Central Index

<sup>173</sup> NPWR is covered under DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization (CLAIMS 3).

<sup>174</sup> SCCLAIMS is a mirror copy of CLAIMS 3 data.

<sup>175</sup> See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>176</sup> See DHS/USCIS/PIA-015 CLAIMS 4 and subsequent updates, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>177</sup> See DHS/USCIS/PIA-056 USCIS ELIS available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>178</sup> See DHS/USCIS/PIA-051 CAMINO, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>179</sup> See DHS/USCIS/PIA-027 RAPS/APSS, and subsequent updates, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>180</sup> See DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program (IDDMP), available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>181</sup> See DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), available at: <http://www.dhs.gov/privacy-impact-assessments>.

System (CIS); National File Tracking System (NFTS)<sup>182</sup> to retrieve the physical locations of A-files; Customer Profile Management System (CPMS)<sup>183</sup> to retrieve data associated with biographic and biometric screening.

*Other Department of Homeland Security (DHS) Component System Interfaces:* IDENT<sup>184</sup> to retrieve data associated with biometric screening; CBP's TECS<sup>185</sup> system, to perform screening, including checks against the FBI, National Crime Information Center (NCIC); ATS-P<sup>186</sup> and UPAX; DHS Watchlist Service<sup>187</sup> for real-time screening against Terrorist Screening Data Base (TSDB) records; and DHS Email as a Service (EaaS) Simple Mail Transfer Protocol (SMTP)<sup>188</sup> server for email.

Additionally, FDNS Officers may manually query several internal and/or external databases or systems to obtain information that may be added to a case in FDNS-DS.

*Other DHS Component Systems Accessed (Manually):* AFI<sup>189</sup>; ADIS<sup>190</sup>; SEVIS<sup>191</sup>; ENFORCE<sup>192</sup> Alien Removal Module.

*External Sources Accessed (Manually):* Department of Labor; DoS; Social Security Administration (SSA) Electronic Verification of Vital Events (EVVE); Federal Aviation Administration websites; Intelligence and law enforcement communities; State and local government agencies; local, county, and state police information networks; state motor vehicle administration databases and websites; driver license retrieval websites; state bar associations; state comptrollers; state probation/parole boards or offices; county appraisal districts; and state sexual predator websites.

---

<sup>182</sup> See DHS/USCIS/PIA-032 National File Tracking System (NFTS) available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>183</sup> See DHS/USCIS/PIA-060 Customer Profile Management Service, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>184</sup> See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>185</sup> See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>186</sup> See DHS/CBP/PIA-006 Automated Targeting System (ATS), available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>187</sup> DHS/USCIS/PIA-027(e) DHS Watchlist Service, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>188</sup> See DHS/ALL/PIA-012 E-mail Secure Gateway and subsequent updates, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>189</sup> See DHS/CBP/PIA-010 AFI, available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>190</sup> See DHS/CBP/PIA-24 Arrival and Departure Information System (ADIS), available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>191</sup> See DHS/ICE/PIA-001(b) Student and Exchange Visitor Information System II (SEVIS), available at: <http://www.dhs.gov/privacy-impact-assessments>.

<sup>192</sup> See DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, available at: <http://www.dhs.gov/privacy-impact-assessments>.

## 4. Efficacy

The 2014-2018 Department of Homeland Security (DHS) Strategic Plan states that DHS will enforce and administer the nation's immigration laws by "ensuring that only eligible applicants receive immigration benefits through expanded use of biometrics, a strengthening of screening processes, improvements to fraud detection, increases in legal staffing to ensure due process, and enhancements of interagency information sharing."<sup>193</sup> ATLAS is a platform that enhances the ability of USCIS FDNS to detect and investigate fraud, national security and public safety concerns, and intelligence threats in forms submitted to USCIS. ATLAS is capable of screening biometric and biographic information associated with forms submitted to USCIS automatically at intake, resolving identities when individuals use aliases, and detecting the relationships among individuals and organizations perpetuating criminal or terrorist activities.

In Fiscal Year 2016 alone, ATLAS screened roughly 12 million combined immigration filing and biometric enrollments and generated over 83,000 SGNs of potential fraud, public safety, and national security concerns, routed to Immigration Officers, which led to more than 5,000 new leads, more than 1,800 findings of fraud, more than 60 confirmed national security concerns, and more than 100 referrals to ICE for possible criminal or enforcement action.

Using ATLAS, application cycle times are greatly reduced, and FDNS Officers are alerted to potential concerns much earlier in the immigration process. In 2015, a subject's fingerprints were taken in association with an application for naturalization, and ATLAS triggered an SGN, alerting FDNS to multiple identities associated with those prints. Further investigation revealed the subject had entered the country illegally on two prior occasions. In both instances, the subject had been apprehended and removed. The investigation also revealed discrepancies in the subject's application for Lawful Permanent Residency. This information, combined with other fraud indicators, led to the subject being placed into immigration proceedings and ultimately being ordered removed by an immigration judge.

ATLAS uses analytical tools to view non-obvious relationships across data and to detect patterns in immigration benefit requests and applications. For example, in 2015, ATLAS generated an SGN for a subject who had used multiple identities and Alien numbers. An FDNS Officer's review revealed the subject had been ordered deported under one identity and again two years later under a second identity. The subject was subsequently paroled into the United States and attempted to file for an adjustment of status under a third identity. Through biometric-based screening, ATLAS was able to resolve the three identities to the same subject, and an FDNS Officer confirmed the subject willfully concealed the prior identities and immigration violations when trying to adjust status. The subject later presented himself to CBP and was ultimately placed into removal proceedings and ordered removed by an immigration judge.

---

<sup>193</sup> Department of Homeland Security. "Fiscal Years 2014 – 2018 Strategic Plan," available at: <https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF>.

## 5. Laws and Regulations

The Immigration and Nationality Act of 1952, as amended (INA), section 103 (8 U.S.C. § 1103) charges the DHS Secretary with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens, including ferreting out incidents of immigration fraud, and for ensuring that individuals who pose national security threats are not granted immigration benefits. The DHS Secretary has delegated to the USCIS Director pursuant to Homeland Security Delegation No. 0150.1, the following duties: (1) to administer the immigration laws (as defined in section 101(a)(17) of the INA); (2) investigate alleged civil and criminal violations of the immigration laws, including but not limited to, alleged fraud with respect to applications or determinations within the BCIS [predecessor to USCIS], and make recommendations for prosecutions, or other appropriate action when deemed advisable.

USCIS has a statutory obligation to ensure that an applicant and/ or beneficiary is admissible in accordance with section 245(a)(2) of the INA.<sup>194</sup> Section 245(a)(2) requires that an alien must be admissible to the United States in order to adjust status to that of a lawful permanent resident. Section 212 of the INA<sup>195</sup> lists several categories of inadmissible aliens. An applicant may be found inadmissible if he or she has been convicted of (or admits to having committed) an offense that constitutes a ‘crimes involving moral turpitude,’<sup>196</sup> or has engaged in or is suspected of engaging in terrorist activities.<sup>197</sup> Similarly, section 237 of the INA<sup>198</sup> sets forth the grounds by which an alien can be determined to be removable or deportable, including a conviction for a crime involving moral turpitude<sup>199</sup> or security and related grounds.<sup>200</sup>

## 6. Privacy Impact and Privacy Protections

FDNS aims to enable effective identification of threats to national security and public safety, detection and combating immigration benefit fraud, and removal of systematic and other vulnerabilities, while respecting individuals’ privacy and promoting transparency of FDNS operations. In May 2016, FDNS updated and re-issued its PIA for the FDNS-DS system<sup>201</sup> to provide public notice of the development of its screening platform, ATLAS, and to provide transparency into the core capabilities planned to be integrated with ATLAS. ATLAS was designed to allow FDNS to optimize the processing of information for the purposes authorized in the INA, while minimizing privacy risks.

<sup>194</sup> INA § 245(a)(2), 8 U.S.C. § 1255, (“Adjustment of status of non-immigrant to that of person admitted for permanent residence”).

<sup>195</sup> *Id.* at § 212, 8 U.S.C. § 1255 (“Inadmissible aliens”).

<sup>196</sup> *Id.* at § 212(a)(2), 8 U.S.C. § 1182(a)(2) (“Criminal and related grounds”).

<sup>197</sup> *Id.* at § 212(a)(3), 8 U.S.C. § 1182(a)(3) (“Security and related grounds”).

<sup>198</sup> *Id.* at § 237, 8 U.S.C. § 1227 (“General classes of deportable aliens.”).

<sup>199</sup> *Id.* at § 237(a)(2), 8 U.S.C. § 1227(a)(2) (“Criminal offense”).

<sup>200</sup> *Id.* at § 237(a)(4), 8 U.S.C. § 1227(a)(4) (“Security and related grounds”).

<sup>201</sup> See DHS/USCIS/PIA-013(a) available at: <http://www.dhs.gov/privacy-impact-assessments>.

FDNS has a vested interest and responsibility to maintain the most accurate data possible since the information could be used in support of an adjudicative decision or in support of criminal investigations undertaken by law enforcement partners. FDNS Officers rely on multiple sources to confirm the veracity of the data and, if discrepancies are uncovered, will take necessary steps to correct inaccuracies. FDNS Officers compare information obtained during the screening and administrative investigation processes with information provided directly by the individual (applicant or petitioner) in the underlying benefit request form or in response to Requests for Evidence or Notices to Appear, to ensure information is matched to the correct individual, as well as to ensure integrity of the data. In the event FDNS Officers learn that information contained within other systems of records is not accurate, the Officer will notify appropriate individuals within the USCIS Records Office or the federal agency owning the data, who will facilitate any necessary notifications and changes.

ATLAS does not collect information directly from individuals. Rather, ATLAS receives information from the individual's form submission and from the associated biographic and biometric-based background checks, which includes information from other DHS and/or USCIS systems. Immigration regulations (8 CFR 103.2(b)(16)) require that individuals be advised of any derogatory information and be given a chance to rebut it, with certain exceptions. Individuals have the opportunity to provide information directly to USCIS throughout the adjudication process in support of their requests or filings. This may occur through interviews, Requests for Evidence, Notices to Appear, or in the form of a Notice of Intent to Deny.

ATLAS's rules-based screening approach is tailored to provide information to FDNS Officers relevant to potential fraud, public safety, and national security threats, and the mere presence of an SGN does not indicate derogatory information about the individual. The SGN process also provides for a layer of human review to confirm SGNs are actionable prior to routing them for further case management activity. FDNS continually monitors and refines rules based on appropriate metrics. FDNS also continually tunes the rules to narrow the scope of information provided to FDNS Officers. Rigorous quality control and assurance procedures are used to adjust rules as necessary to reduce the potential for false positives. The rules help standardize how information is analyzed and help to detect patterns, trends, and risks that are not easily apparent from the form submissions themselves.

FDNS-DS maintains strict access controls so that only FDNS-DS users with a role in investigating cases for potential fraud, public safety, and national security concerns have access to raw data retrieved as part of the screening process. ATLAS interfaces with other systems to help streamline the processes that FDNS-DS users currently perform manually, and its capabilities are designed to assist FDNS Officers in obtaining information needed to confirm an individual's eligibility for the benefit or request sought while preserving the integrity of the legal immigration system. The output to other case management systems is reasonably tailored to provide adjudications staff with information relevant to making a determination on the benefit or request sought.

In order to reduce the risk of new data being incorporated into FDNS that has not been reviewed for privacy and legal concerns, multiple layers of privacy and legal review have been built into

FDNS's processes. Additionally, FDNS must submit a privacy threshold analysis and receive approval from the DHS Privacy Office before adding any new data sources.

Because FDNS-DS contains sensitive PII related to possible immigration benefit fraud and national security concerns, DHS has exempted FDNS from the notification, access, and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(k)(2). Notwithstanding the applicable exemptions, USCIS reviews all such requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of USCIS, and in accordance with procedures and points of contact published in the applicable SORNs.

## **IV. CONCLUSIONS**

The DHS Privacy Office is pleased to provide the Congress its eleventh 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 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	
ABIS	Department of Defense Automated Biometric Identification System
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-L	Automated Targeting System—Land Module
ATS-N	Automated Targeting System—Inbound Module
ATS-P	Automated Targeting System— Passenger
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
CEI	Common Entity Index
CMAA	Customs Mutual Assistance Agreement
CMIR	The Report of International Transportation of Currency or Monetary Instruments Report
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
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
EVUS	Electronic Visa Update System
FALCON-SA	FALCON Search & Analysis
FBI	Federal Bureau of Investigation
FDNS	Fraud Detection and National Security Directorate

Acronym List	
FDNS-DS	Fraud Detection and National Security – Data System
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
IDENT	Automated Biometric Identification System
IFS	Intelligence Fusion System
INA	Immigration and Nationality Act
IOC	Interagency Operations Center
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAA	Information Sharing and Access Agreement
IT	Information Technology
LES	Law Enforcement Sensitive
MOA	Memorandum of Agreement
MSB	Money Services Business
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NIIS	Non-immigrant 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
RAPS	Refugee, Asylum, and Parole System
RFI	Request for Information
SAFE Port Act	Security and Accountability for Every Port Act
SANS	Ship Arrival Notification System
SAVI	Suspect and Violator Indices
SBU	Sensitive But Unclassified
SDN	Specially Designated National
SELC	System Engineering Life Cycle
SEVIS	Student and Exchange Visitor Information System
SGN	System Generated Notification
SORN	System of Records Notice

Acronym List	
SSN	Social Security number
SSI	Sensitive Security Information
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TSC	FBI Terrorist Screening Center
TSDB	Terrorist Screening Database
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