# DHS Privacy Office

## 2019 Data Mining Report to Congress

*December 2, 2020*

Homeland Security

## Foreword

*December 2, 2020*

I am pleased to present the U.S. Department of Homeland Security's (DHS) 2019 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 activities, 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 activities impact on privacy and the protections in place to protect privacy. This is the fourteenth comprehensive DHS Data Mining Report and the twelfth report prepared pursuant to the Act. Three annexes to this report, containing Law Enforcement Sensitive information, are 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 to meet Departmental goals and objectives. Consistent with the rigorous compliance process it applies to all DHS programs and systems, the DHS Privacy Office works closely with the programs discussed in this report to ensure they employ data mining in a manner that supports the Department's mission to protect the homeland and protects privacy.

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

Sincerely,

Dena Kozanas
Chief Privacy Officer and Chief FOIA Officer
U.S. Department of Homeland Security

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

**The Honorable Michael Pence**
President, U.S. Senate

**The Honorable Nancy Pelosi**
Speaker, U.S. House of Representatives

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

**The Honorable Gary Peters**
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

**The Honorable Lindsey Graham**
Chairman, U.S. Senate Committee on the Judiciary

**The Honorable Dianne Feinstein**
Ranking Member, U.S. Senate Committee on the Judiciary

**The Honorable Marco Rubio**
Chairman (Acting), U.S. Senate Select Committee on Intelligence

**The Honorable Mark Warner**
Vice Chairman, U.S. Senate Select Committee on Intelligence

**The Honorable Richard Shelby**
Chairman, U.S. Senate Committee on Appropriations

**The Honorable Patrick Leahy**
Vice Chairman, U.S. Senate Committee on Appropriations

**The Honorable Mike Crapo**
Chairman, U.S. Senate Committee on Banking, Housing, and Urban Affairs

**The Honorable Sherrod Brown**
Ranking Member, U.S. Senate Committee on Banking, Housing and Urban Affairs

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

**The Honorable Mike Rogers**
Ranking Member, U.S. House of Representatives Committee on Homeland Security

**The Honorable Carolyn Maloney**
Chairwoman, U.S. House of Representatives Committee on Oversight and Reform

**The Honorable James Comer**
Ranking Member, U.S. House of Representatives Committee on Oversight and Reform

**The Honorable Jerrold Nadler**
Chairman, U.S. House of Representatives Committee on the Judiciary

**The Honorable Jim Jordan**
Ranking Member, U.S. House of Representatives Committee on the Judiciary

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

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

**The Honorable Nita M. Lowey**
Chairwoman, U.S. House of Representatives Committee on Appropriations

**The Honorable Kay Granger**
Ranking Member, U.S. House of Representatives Committee on Appropriations

**The Honorable Maxine Waters**
Chairwoman, U.S. House of Representatives Committee on Financial Services

**The Honorable Patrick McHenry**
Ranking Member, U.S. House of Representatives Committee on Financial Services

## Table of Contents

## I. Executive Summary

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

In the 2018 DHS Data Mining Report,[2] 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 Import Cargo) and outbound (ATS-AT) cargo, passengers (ATS-P), land border crossings (ATS-L), and;
- 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;
- The DHS Data Framework, which is a DHS-wide initiative;
- The SOCRATES Pilot Program, which is administered by CBP; and
- The Fraud Detection and National Security – Data System (FDNS-DS)/ATLAS, which is administered by the U.S. Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security Directorate (FDNS).

This year's report, covering the period of January 1 through December 31, 2019, provides updates on additions, modifications, and other developments to the above referenced programs. In addition, the DHS Privacy Office identified two additional Departmental programs that engages in data mining, as defined by the Act:

- The Global Command and Control System – Joint (GCCS-J), which is administered by the United States Coast Guard (USCG); and
- The Unclassified Common Operating Picture (UCOP) administered by the USCG.

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

[1] 42 U.S.C. § 2000ee-3.
[2] 2018 DHS Data Mining Report, issued in November of 2019, available at: https://www.dhs.gov/sites/default/files/publications/2018-dataminingreport.pdf.

The *Homeland Security Act of 2002* expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[3] DHS exercises this authority with respect to the programs discussed in this report, all of which have been reviewed for its potential impact on privacy by the DHS Chief Privacy Officer.

The Chief Privacy Officer's authority for evaluating DHS data mining activities stems from 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."[4]

The DHS Privacy Office implements the Chief Privacy Officer's authorities through privacy compliance policies and procedures based on a set of eight Fair Information Practice Principles (FIPPs) and is rooted in the tenets of the Privacy Act.[5] The FIPPs serve as DHS' core privacy framework and are memorialized in the DHS 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 U.S. Department of Homeland Security (December 29, 2008)*[6] *and in several Department-wide directives including, Directive 047-01, Privacy Policy and Compliance.*[7]

As described more fully below, the DHS Privacy Office's privacy compliance process requires components and offices that use systems and manage programs that collect, ingest, maintain, and use Personally Identifiable Information (PII) and other information relating to individuals to complete privacy compliance documentation, such as a Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and Systems of Records Notices (SORNs). Submission of the PTA enables the DHS Privacy Office to determine whether a Department program or system effects privacy, and if so, whether additional privacy compliance documentation is required. Additional privacy documentation could include the publication of a PIA, required by the *E-Government Act of 2002*[8] and/or the Chief Privacy Officer's authorities,[9] as well as a SORN, required by the *Privacy Act of 1974*,[10] both of which are required before a program can 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 covered by DHS SORNs as well.

---

[3] 6 U.S.C. § 121(d)(11).
[4] 6 U.S.C. § 142(a)(1).
[5] 5 U.S.C. § 552a.
[6] Privacy Policy Directive 140-06 and Privacy Policy Guidance Memorandum 2017-01, *available at*: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf and https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.
[7] Directive 047-01 and its accompanying Instruction *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf and https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf, respectively.
[8] 44 U.S.C. § 3501, note Section 208 of the E-Government Act.
[9] 6 U.S.C. § 142(a)(4).
[10] 5 U.S.C. § 552a(e)(4).

While each program described below engages in data mining to some extent, the DHS Privacy Office has validated that no decisions regarding 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 in making determinations about individuals who may have been initially identified through data mining activities. The DHS Privacy Office works closely with each of these programs to ensure that the required privacy compliance documents are current, personnel receive appropriate privacy training and privacy protections are implemented and followed.

## II. Legislative Requirement

The Federal Agency Data Mining Reporting Act of 2007, at 42 U.S.C. § 2000ee-3(c), includes the following reporting 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 ([1]) 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.

3. Annex

(A) In general

A report under subparagraph ([1]) shall include in an annex any necessary--

(i) classified information;

(ii) law enforcement sensitive information;

(iii) proprietary business information; or

(iv) trade secrets (as that term is defined in section 1839 of Title 18).

(B) Availability

Any annex described in clause ([A])—

(i) shall be available, as appropriate, and consistent with the National Security Act of 1947, to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Financial Services of the House of Representatives; and

(ii) shall not be made available to the public.

4. Time for Report

Each report required under subparagraph ([1]) shall be—

(A) submitted not later than 180 days after August 3, 2007; and

(B) updated not less frequently than annually thereafter, to include any activity to use or develop data mining engaged in after the date of the prior report submitted under subparagraph ([1]).

The Act, at 42 U.S.C. § 2000ee-3(b)(1), 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—
>
> a) the detection of fraud, waste, or abuse in a Government agency or program;
>
> or
>
> b) the security of a Government computer system.[11]

[11] "[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.

## III. Data Mining Use and the DHS Privacy Compliance Process

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 Policy Guidance Memorandum 2017-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the U.S. Department of Homeland Security (December 29, 2008)[12] and in Department-wide directives including Directive 047-01, Privacy Policy and Compliance.[13] The FIPPs govern the appropriate collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) at the Department in fulfilment of the Department's mission to preserve, protect, and secure the homeland. The DHS Privacy 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);[14] (2) the Privacy Impact Assessment (PIA);[15] and (3) the System of Records Notice (SORN).[16] Each of these documents has a distinct function in the DHS privacy compliance framework. Together, they promote transparency and demonstrate accountability.

To fulfill the requirements under the Act, the DHS Privacy Office identifies DHS programs that engage in data mining through its routine compliance oversight activities as well as targeted activity questionnaires focusing on data mining attributes. Additionally, the DHS Privacy Office reviews all of the Department's IT budget submissions to the Office of Management and Budget (OMB) to gain knowledge of programs or systems that use PII and to determine whether they address privacy appropriately.[17] The DHS Privacy Office also evaluates PTA submissions to review all information

---

[12] Privacy Policy Directive 140-06 and Privacy Policy Guidance Memorandum 2017-01, *available at*: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf and https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

[13] Directive 047-01 and its accompanying Instruction *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf and https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf respectively.

[14] The DHS privacy compliance process begins with a PTA, a required document by DHS policy that serves as the official determination by the DHS Privacy Office as to whether a Department program or system has privacy effects, and if additional privacy compliance documentation is required, such as a PIA and/or SORN. Additional information concerning PTAs is available at: https://www.dhs.gov/privacy.

[15] The E-Government Act of 2002 requires federal agencies to publish PIAs when there are new electronic collections of, or new technologies applied to, PII. 44 U.S.C. § 3501 note. *See also* OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act." As a matter of policy, DHS extends this requirement to all programs, systems, and activities that involve PII or are otherwise privacy-sensitive, pursuant to the Chief Privacy Officer's authority under 6 U.S.C. § 142.

[16] 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), (e)(4).

[17] 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, Preparation, Submission, and

technology systems that are going through the security authorization process required by the Federal Information Security Modernization Act of 2014 (FISMA)[18] to determine whether they maintain PII. Furthermore, its PTA/PIA process provides the DHS Privacy Office additional insight into technologies used or intended to be used by DHS. Collectively, these oversight activities provide the DHS Privacy Office multiple opportunities to identify proposed data mining activities and then engage program managers in discussions about potential privacy issues.

The DHS Privacy Office has worked closely with the relevant DHS Components to ensure that privacy compliance documentation required for each program described in this report is current. All the programs identified herein have either issued new PIAs or are in the process of updating current PIAs; all programs are also covered by DHS SORNs.

Execution of the Budget, *available at*: https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf.

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

## IV. Reporting

In the 2018 DHS Data Mining Report,[19] the DHS Privacy Office discussed the following Departmental programs that engaged 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 Import Cargo) 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;
- The DHS Data Framework, which is a DHS-wide initiative;
- The SOCRATES Pilot Program, which is administered by CBP; and
- The Fraud Detection and National Security – Data System (FDNS-DS)/ATLAS, which is administered by the U.S. Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security Directorate (FDNS).

This section of the 2019 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, the DHS Privacy Office identified two additional Departmental programs that engage in data mining, as defined by the Act:

- The Global Command and Control System – Joint (GCCS-J), which is administered by the United States Coast Guard (USCG); and
- The Unclassified Common Operating Picture (UCOP) administered by the USCG.

DHS also provides three annexes to this report, which include Law Enforcement Sensitive Information, to Congress as required by the Act.

### A. Automated Targeting System (ATS)

CBP operates the ATS decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data. ATS runs risk-based rules, predictive analytics, and queries to identify patterns indicative of terrorist or criminal activity. Certain targeting activities are derived from derogatory information about known or suspected terrorists (KST). During the 2017 reporting period and in furtherance of the program, CBP published an ATS PIA[20] update to notify the public of additional populations that ATS will vet. The

[19] 2018 DHS Data Mining Report, *available at* https://www.dhs.gov/sites/default/files/publications/2018-dataminingreport.pdf.

[20] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates, *available at:*

expanded populations include: Secure Flight Passenger Data,[21] Trusted Travelers and Trusted Workers, immigration benefit applicants and petitioners, international aviation crew members, and CBP employees and applicants. During the 2019 reporting period, CBP made no modifications or updates to the vetting of these populations.

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

As described in the 2012 ATS PIA[22], subsequent PIA updates, and reported in the previous DHS Data Mining Reports,[23] 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 vetting for non-immigrant visas. In Fiscal Year (FY) 2017, DoS began sending immigrant visa applications for vetting to CBP using the same process as non-immigrants. 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)[24] indicating whether DHS has identified derogatory information about the individual based on risk-based rules. Applications of individuals for whom derogatory information is identified are vetted in two ways. The applications 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)[25] case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD. The *Enhanced Border Security and Visa Entry Reform Act of 2002* (EBSVERA) authorizes the use of ATS-P for screening non-immigrant and immigrant visas.[26]

### 2) Overstay Vetting

The goal of the Overstay Vetting effort is to allow ICE to deploy its investigative resources more efficiently to locate high-risk overstays and initiate criminal investigations or removal proceedings against those overstay individuals. The Overstay Hotlist (leveraged by the Overstay Vetting employees) is a list of overstay leads derived from data obtained through ATS and is used to develop investigative priorities based on associated risk patterns linked to national security and public safety factors. This prioritized list of overstay leads is then passed on to ICE's LeadTrac[27]

---

https://www.dhs.gov/privacy.

[21] Pursuant to 49 CFR § 1560.3 Secure Flight Passenger Data or (SFPD) means information regarding a passenger or non-traveling individual that a covered aircraft operator or covered airport operator transmits to TSA, to the extent available, pursuant to § 1560.101. SFPD is the following information regarding a passenger or non-traveling individual: (1) Full name, (2) Date of birth, (3) Gender, (4) Redress number or Known Traveler Number (once implemented), (5) Passport information, (6) Reservation control number, (7) Record sequence number, (8) Record type, (9) Passenger update indicator, (10) Traveler reference number, and (11) Itinerary information.

[22] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates, *available at* https://www.dhs.gov/privacy.

[23] Originally published in the 2013 DHS Data Mining Report, *available at:* https://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf.

[24] *See* the CCD PIA, *available at:* https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf.

[25] *See* DHS/ICE/PIA-011 Visa Security Program Tracking System (VSPTS-Net), *available at:* https://www.dhs.gov/privacy.

[26] Pub. L. No. 107-173, codified as amended in 8 U.S.C. §§ 1701 – 1778 (2018).

[27] 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

system for further investigation and possible enforcement action.

In addition to prioritizing overstay leads, ATS is also used to vet overstay candidates received from DHS/CBP's Arrival and Departure Information System (ADIS),[28] in an effort to identify potential information related to visa overstay candidates derived from supporting data available from other source systems, including ATS, i.e., border crossing information (derived from DHS/CBP's Border Crossing Information (BCI) system),[29] Form I-94 Notice of Arrival/Departure records (derived from DHS/CBP's Nonimmigrant Information System (NIIS)),[30] and data from the DHS/ICE Student Exchange Visitor Information System (SEVIS).[31]

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.[32]

### 3) Trusted Traveler and Trusted Worker Vetting

The vetting process for CBP's Trusted Traveler Programs and Trusted Worker populations 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, Trusted Worker, and Registered Traveler Program applicants. CBP Officers analyzed and assessed this data to be utilized during the enrollment interview. The ATS Trusted Traveler Vetting Program and Trusted Worker Program are modernized versions of VCM.

In October 2016, all targeting for new and updated Trusted Traveler applications were 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 National Law Enforcement Telecommunications System (NLETS) queries.[33] ATS provides

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-015 LeadTrac SORN, (August 9, 2016) 81 Fed. Reg. 52700, *See* DHS/ICE/PIA-044 LeadTrac System *available at:* http://www.dhs.gov/privacy.

[28] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, DHS/CBP-021 Arrival and Departure Information System (ADIS), (November 18, 2015) 80 Fed. Reg. 7208, DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates and DHS/ALL/PIA-041 One DHS Overstay Vetting Pilot *available at:* http://www.dhs.gov/privacy.

[29] DHS/CBP-007 Border Crossing Information (BCI) SORN, 81 Fed. Reg. 89957 (December 13, 2016).

[30] DHS/CBP-016 Nonimmigrant Information System, 80 Fed. Reg. 13398 (March 13, 2015).

[31] *See* DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) *available at:* http://www.dhs.gov/privacy and DHS/ICE-001 Student and Exchange Visitor Information System, (January 5, 2010) 75 Fed. Reg. 412.

[32] A complete list of authorities is included in the PIA for the Overstay Vetting Pilot, *available at*: https://www.dhs.gov/privacy.

[33] 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

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. In FY 2017, CBP enabled a recurrent vetting process beyond the initial submission for trusted travelers through the ATS platform. Additionally, since FY 2017, CBP enabled Ports of Entry to use the ATS platform to vet Trusted Worker applicants.

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.*

#### 4) Special ATS Programs

##### a.) ATS Enhancements to Watchkeeper System

Watchkeeper is the United States Coast Guard's (USCG) information sharing and management system software for Interagency Operations Centers (IOC). The USCG established Watchkeeper to improve multi-agency maritime security operations and enhance cooperation amongst 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.

The USCG enhanced Watchkeeper by integrating the ATS Import Cargo and ATS-P modules, discussed below, as tools to conduct pre-arrival screening and vetting of vessel cargo, crew, and passengers. 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's 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.*

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).

*§ 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.[34]

### b.) 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.[35] 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 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,[36] 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 Import Cargo 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 Import Cargo and ATS-AT[37] became operational in 1997. ATS-P (the new User

[34] *See* DHS/USCG/PIA-020 Interagency Operations Center (IOC) Watchkeeper, *available at*: https://www.dhs.gov/privacy.

[35] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates *available at* https://www.dhs.gov/privacy.

[36] *See* DHS/CBP/PIA-020 Export Information System (EIS), *available at* https://www.dhs.gov/privacy. 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 way 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.

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

Interface is now referred to as Unified Passenger, or UPAX)[38] 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 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).[39]

ATS ingests various data in real-time from the following DHS and CBP systems: Automated Commercial System (ACS), Advance Passenger Information System (APIS), Automated Commercial Environment (ACE), Electronic System for Travel Authorization (ESTA), Electronic Visa Update System (EVUS),[40] Global Enrollment System (GES), the Nonimmigrant Information System (NIIS), BCI, Seized Asset and Case Tracking System (SEACATS), ICE's SEVIS and Enforcement Integrated Database (EID), and TECS.[41] TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[42] Terrorist Screening Database (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 Import Cargo. 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.

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

[39] 49 U.S.C. § 44909. The regulations implementing the PNR provisions of ATSA are codified at 19 C.F.R. § 122.49d.

[40] In October 2016, as described in the 2016 data mining report, CBP began vetting Electronic Visa Update System (EVUS) applications in 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. DHS and DoS established EVUS under the authority granted in the Immigration and Nationality Act (INA). 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. CBP has no modifications or updates to EVUS in the FY 2017 reporting period.

[41] PIAs for these programs are *available at* https://www.dhs.gov/privacy.

[42] 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.

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.

Many 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.

### i) ATS Import Cargo and Automated Export System (AES) Modules

#### 1. Program Description

ATS Import Cargo assists CBP officers in identifying and selecting for additional inspection inbound cargo shipments that pose a risk of containing goods that may violate U.S. law. ATS Import Cargo is available to CBP officers at all ports of entry (i.e., air, land, sea, and rail) and assists CBP personnel in the Container Security Initiative and Secure Freight Initiative with decision-making processes.

The functionality of ATS-AT was modernized in 2014 when the Export Cargo Targeting system was re-engineered and deployed by CBP. Rebranded as the Automated Export System (AES), the system aids CBP officers in identifying export shipments that pose a high risk of containing goods that 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 Import Cargo and AES examine data related to cargo in real time and engage in data mining to provide decision support analysis for the targeting of cargo for possible violations of U.S. law. The cargo analysis provided by these platforms is intended to add automated anomaly detection to CBP's existing targeting capabilities, and to enhance screening of cargo prior to its arrival into or departure from the United States.

## 2. Technology and Methodology

ATS Import Cargo and AES do not collect information directly from individuals. The data used in the development, testing, and operation of ATS Import Cargo and AES screening technology is taken from bills of lading and shipping manifest data provided to CBP 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 Import Cargo and AES are used to identify goods that may need additional scrutiny for national security purposes and to ensure compliance with U.S. law. No decisions about individuals are made solely based on these automated results.

The Security and Accountability For Every (SAFE) Port Act requires CBP to consider the use of advanced algorithms in support of its mission.[43] To that end, as discussed in previous DHS Data Mining Reports, CBP established an Advanced Targeting Initiative (ATI), which employs the development of data mining, machine learning,[44] and other analytic techniques to enhance ATS Import Cargo and AES. This initiative strives to improve law enforcement capabilities with predictive models and establish performance evaluation measures to assess the effectiveness of ATS screening for inbound and outbound cargo shipments across multimodal conveyances.

Current efforts seek to augment existing predictive models by expanding the use of feedback from certain identified 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 whether additional scrutiny is needed. Additionally, CBP continues to develop and test machine learning models or 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.

ATI is part of ATS's maintenance and operation of the ATS Import Cargo and AES. The design and tool-selection processes for data mining, pattern recognition, and machine learning techniques under development in ATI are being evaluated through user acceptance testing by the National Targeting Center-Cargo Division (NTC-CD). The NTC-CD and the CBP Office of Intelligence further support the performance of research on entities and individuals of interest, data queries, and various analysis techniques 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.

## 3. Data Sources

Since, ATS Import Cargo and AES do not collect information directly from individuals, the

[43] 6 U.S.C. § 943(e)(2).

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

information is either submitted by private entities or persons and initially collected in DHS/CBP source systems (e.g., ACE). This data collection is 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 Import Cargo and AES use data from source systems to gather information about importers and exporters, cargo, and conveyances used to facilitate the importation of cargo into and the exportation of cargo out of the United States. This information includes PII concerning individuals associated with imported and exported cargo (e.g., brokers, carriers, shippers, buyers, consignees, sellers, exporters, freight forwarders, and crew). ATS Import Cargo 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.[45] 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 present various information as another method to detect cargo that may need additional scrutiny. CBP also uses custom-designed software to resolve ambiguities related to inbound and outbound cargo.

### 4. Efficacy

Based on the results of testing and operations in the field, ATS Import Cargo and AES have proven to be effective means of identifying suspicious cargo that requires further investigation by CBP officers. The results of ATS Import Cargo and AES 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 have used ATS-Import Cargo to identify, through risk-based rule sets, cargo shipments and commodities that were referred for further examination. For example, on April 9, 2019, CBP seized 12 kilograms of opium based on an NTC-CD referral. NTC-CD identified the shipment from Turkey transiting the United States to Canada as a match to a user defined rule (UDR) and high risk for narcotic smuggling.

Additionally, on July 19, 2019, a CBP port of entry seized electronic components based upon a referral from NTC-CD due to a match to an outbound counterproliferation user defined rule (UDR) within AES.

### 5. 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.[46] AES and ATS Import Cargo 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

[45] ATS-N collects information from source systems regarding individuals in connection with for example, bills of lading.
[46] *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.

for counterterrorism and drug law enforcement. AES also supports functions arising from the Anti-Terrorism Act of 1987[47] and the 1996 Clinger-Cohen Act.[48] The risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.[49]

### ii) ATS-Passenger (ATS-P)

#### 1. Program Description

ATS-P is a custom-designed system used at U.S. ports of entry, particularly those receiving international flights (both commercial and private) and voyages, 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. 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 United States because that person may pose a greater risk for terrorism and related crimes or other crimes. ATS-P is a fully operational application that utilizes CBP's System Engineering Life Cycle methodology[50] and is subject to recurring systems maintenance.

#### 2. Technology and Methodology

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. It applies 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 vetting and inspection process. This presentation involves providing direct access to cross-referenced files and information from partner agency databases using 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

[47] 22 U.S.C. §§ 5201 *et seq.*
[48] 40 U.S.C. §§ 1401 *et seq.*
[49] 6 U.S.C. § 912(b).
[50] 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.

records, warrants, and patterns of suspicious activity identified through past investigations. The results of these comparisons are either assessments of the risk-based rules or 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 law enforcement and intelligence databases, 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 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 CBP officers in identifying illegal activity or possible admissibility issues. 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.

### 3. Data Sources

ATS-P uses information available in ATS to assist in the development of the risk-based rules discussed above.

### 4. 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 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 trafficking and smuggling operations. For example, CBP officers working at the NTC using ATS-P identified an individual

departing the United States, who was wanted by local authorities for sexual assault and endangering the welfare of a child. Based on the research conducted by the NTC, the subject was referred for an outbound inspection as he attempted to depart the United States, was subsequently detained and turned over to the local law enforcement officers. In addition, CBP officers working at the NTC using ATS-P identified an inbound international traveler as a high-risk for fraud. NTC coordinated with the airline prior to the traveler boarding a plane departing for the United States. Based on the information provided by NTC, airline security officers, in coordination with airport police, determined the traveler was in possession of a fraudulent passport. The traveler was denied boarding by the airline at the foreign airport. Airport police took custody of the traveler and seized the altered passport.

#### 5. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.[51] 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,[52] ATSA, IRTPA, the Immigration and Nationality Act (INA), and the Tariff Act of 1930, as amended.[53] 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.

### iii) ATS-Land Module (ATS-L)

#### 1. 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.

#### 2. 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) to identify travelers

[51] *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.
[52] 8 U.S.C. § 1721.
[53] 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.

who may need additional scrutiny ATS-L also compares license plate and DMV data to information in ATS source databases including; watch lists, criminal records, and warrants. The results of these comparisons assist officers in determining whether additional scrutiny is warranted, and they also facilitate travel.

The results of positive queries in ATS-L are designed to signal to the 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 offer another tool to officers and agents and facilitate the development of a recommendation prior to the person or vehicle's arrival at the point of initial inspection. 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.

### 3. Data Sources

ATS-L uses and relies upon information available in ATS to assist in the development of the risk-based rules discussed above.

### 4. 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, on May 16, 2019, ATS-L provided information to CBP which resulted in the referral of a vehicle with a Mexican Citizen at a land port of entry. The CBP inspection identified a non-factory compartment in the rear doors of the vehicle that held 138 plastic-wrapped packages inside containing 70.82 kilograms of methamphetamine and 2.84 kilograms of fentanyl. CBP seized the contraband and arrested the subject who was turned over to Homeland Security Investigations (HSI) for federal prosecution.

### 5. Laws and Regulations

CBP is responsible for collecting and reviewing information about vehicles and their occupants prior to entering the United States.[54] As part of this inspection and examination process, all vehicles

[54] *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

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.

#### iv) TSA Silent Partner and Quiet Skies Programs

##### 1. Program Description

The Transportation Security Administration (TSA) leverages its access to CBP's ATS to identify individuals for enhanced screening during air travel through use of rules based on current intelligence as part of its Secure Flight vetting process. As described in the TSA Silent Partner and Quiet Skies PIA[55], these programs add another layer of risk-based security by identifying individuals who may pose an elevated security risk in addition to individuals on other watch lists maintained by the Federal Government, so that TSA can take appropriate actions to address and mitigate that risk.

Under Silent Partner, TSA creates rules based on current intelligence for use by ATS to identify passengers for enhanced screening on their international flights bound for the United States. Once identified by the rule, those passengers are placed on a Silent Partner List that is retained for the period of the international in-bound flight. Quiet Skies rules are a subset of the Silent Partner rules that are aligned to potential aviation security threats within the United States. TSA uses Quiet Skies rules to create a temporary Quiet Skies List to designate passengers who fall within the Quiet Skies subset of rules for enhanced screening on some subsequent domestic and outbound international travel. The Silent Partner List and Quiet Skies List change daily as individuals are added and deleted.

TSA formulates rules for Silent Partner and Quiet Skies to address unknown and partially identified threats. The risk-based, intelligence-driven rules are not used to deny boarding but result in a limited number of individuals being identified for enhanced screening and may result in other operational response including observation by the TSA Federal Air Marshal Service (FAMS) while the individual is aboard a flight or in the airport. Individuals matching Silent Partner and Quiet Skies rules are not considered "known or suspected terrorists" and are not nominated to the Terrorist Screening Database (TSDB) under Homeland Security Presidential Directive 6 merely for having travel that falls within a security rule. They may be nominated to the TSDB, however, if they are involved in a security incident that would support such nomination.

##### 2. Technology and Methodology

The Silent Partner and Quiet Skies programs utilize CBP's ATS to create lists of aviation

U.S.C. § 46501; and 49 U.S.C. § 44909.

[55] *See* DHS/TSA/PIA-018(i) Secure Flight - Silent Partner and Quiet Skies. *available at* https://www.dhs.gov/privacy.

passengers selected for enhanced screening based on risk-based intelligence-driven rules as part of TSA's Secure Flight program vetting process. The rules are based on aggregated travel data, intelligence, and trend analysis of the intelligence and suspicious activity. Travelers may match a Silent Partner or Quiet Skies rule based upon travel patterns matching intelligence regarding terrorist travel; upon submitting passenger information matching the information used by a partially identified terrorist; or upon submitting passenger information matching the information used by a Known or Suspected Terrorist.

### 3. Data Sources

The information used by the system is initially provided by the individual passengers to airlines (or to reservations agents). ATS collects and retains information about passengers entering or departing the United States in accordance with United States legal requirements on individuals who make reservations for airline travel. This data includes passenger manifests (through APIS, which also includes crew data for flights overflying the United States), immigration control information, and Passenger Name Record (PNR) data. The PNR data may include such items as name, address, email address, phone number, flight, seat number, and other information collected by the airline in connection with a particular reservation. Not all air carriers capture the same amount of information; the number of items captured may even vary among individual PNRs from the same carrier. Information that may be passed by ATS to TSA includes: ATS Passenger ID; full name; date of birth; country where passport was issued; passport number; country of birth; departure date; departure airport; arrival airport; airline code; and Rules ID identifying the rule that was triggered. When an individual matches one or more Silent Partner or Quiet Skies rules, ATS transmits the passenger's Secure Flight Passenger Data and an identifier for the rule or rules matched to Secure Flight for placement on the Silent Partner List or Quiet Skies List, as appropriate. In addition, as authorized ATS users, TSA can access additional information about an individual that may be contained within ATS including the data elements leading to the rule match, as well as phone numbers, credit card information, reservation agent information, prior encounter information, and other information within ATS.

Secure Flight collects and retains full name, date of birth, gender, redress number (if available), known traveler number (if implemented and available), and passport information (if available) for domestic flights and international flights arriving in, departing from, or overflying the continental United States (defined as the 48 lower contiguous states), as well as international flights operated by U.S. carriers. Secure Flight will maintain the Silent Partner List and Quiet Skies List, as well as a record of individuals who matched the Silent Partner List and Quiet Skies List during their travel.

### 4. Efficacy

On December 25, 2009, Umar Farouk Abdulmutallab made a failed attempt to detonate an explosive device while on board Flight 253 from Amsterdam to Detroit. Mr. Abdulmutallab was not in the TSDB. As a result of this attack, TSA conducted a review of the existing threats to aviation security and determined that it needed to implement additional measures to mitigate the threat to commercial aviation posed by unknown or partially known terrorists, based on analysis of current intelligence on terrorist travel and tradecraft. The Silent Partner and Quiet Skies Programs, developed based on results derived from the reviews conducted, designate higher risk passengers

using intelligence-based rules, ensuring enhanced screening of such passengers prior to boarding flights to and within the United States.

As one example, Silent Partner identified for enhanced screening a partially identified terrorist who used biographic information not contained within the TSDB and would not otherwise have been watchlisted or designated for enhanced screening. This individual was subsequently arrested due to suspicion that he was conducting pre-attack surveillance within the Homeland for a foreign terrorist organization. Additionally, TSA conducted an analysis of passengers designated for enhanced screening by Quiet Skies and found that some passengers had been independently added to the TSDB as Known or Suspected Terrorists (KST) subsequent to being designated for enhanced screening by Quiet Skies. Because TSA does not use Silent Partner or Quiet Skies to nominate individuals to the TSDB, these additions came by some means other than TSA action or analysis. While matching a Silent Partner or Quiet Skies rule does not indicate that any particular individual should be placed in the TSDB, this analysis indicates that rules successfully identify passengers whose travel indicates a higher than normal risk.

## 5. Laws and Regulations

TSA's general operating authorities are set forth in the *Aviation and Transportation Security Act (ATSA), 49 U.S.C. § 114(d)-(f).* In addition, the I*ntelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),* specifically directs TSA to test and implement a pre-flight passenger prescreening program, such as *Secure Flight. Section 4012(a)(1) of the IRTPA (codified at 49 U.S.C. § 44903(j)(2))* requires TSA to assume from air carriers the comparison of passenger information for domestic flights to the consolidated and integrated terrorist watch list maintained by the *Federal Government. Section 4012(a)(2) of IRTPA (codified at 49 U.S.C. § 44909(c))* similarly requires the DHS to compare passenger information for international flights to and from the United States against the consolidated and integrated terrorist watch list before departure of such flights.

Pursuant to 49 U.S.C. § 114(f)(2), TSA is required to assess threats to transportation. In addition to screening against the No Fly and Selectee watch lists, when warranted by security considerations, TSA may screen against the full TSDB or other records. TSA has authority under 49 U.S.C. § 114(f) to receive, assess, and distribute intelligence information related to transportation security; to assess threats to transportation; to develop polices, strategies, and plans for dealing with threats to transportation security; and to carry out such other duties and exercise such other powers relating to transportation security as the Administrator considers appropriate. The development of these rules-based programs and integration with Secure Flight were established by TSA to address specific changes observed in how potential terrorists moved from initial radicalization and recruitment to operational readiness. Section 1949 of the FAA Reauthorization Act of 2018 establishes statutory requirements regarding the review of and oversight for TSA's intelligence-driven, risk-based screening rules, and requires TSA and the DHS Traveler Redress Inquiry Program to ensure the availability of the redress process for passengers impacted by TSA's screening rules. Section 1949 further specifies that FAMS shall take these screening rules into account for mission scheduling purposes. Further, pursuant to recommendations by the Government Accountability Office, as reflected in Section 1959 of the FAA Reauthorization Act of 2018, FAMS are required to use a risk-based strategy when allocating resources for international and domestic flight coverage.

Incorporating Silent Partner and Quiet Skies into the FAMS deployment strategy enables TSA to meet the risk-based approach required by Congress and further mitigate potential risk across encounters with the same individual during his or her travel lifecycle.

### 6. ATS Privacy Impacts and Privacy Protections

The DHS Privacy Office works 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,[56] and updated the SORN for ATS in May 2012.[57] 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, 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.[58] 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 assist CBP officers and analysts in either refining their analysis or formulating queries to obtain additional information upon which to base decisions or actions regarding individuals crossing U.S. borders.

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

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 act to correct that information, as appropriate. ATS monitors source systems for changes to the source system

[56] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates *available at* https://www.dhs.gov/privacy.
[57] DHS/CBP-006 Automated Targeting System, (May 22, 2012) 77 Fed. Reg. 30297.
[58] Personnel from TSA, ICE, USCIS, USCG, and DHS's 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.

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, EVUS, 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.[59]

When 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 data subject has access to the redress process, which was previously developed by DHS. The data subject is provided information about the redress process during examination at secondary inspection. In addition, CBP officers have a brochure available for individuals 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.[60] CBP created the CBP INFO Center in its Office of Public Affairs to serve as a clearinghouse for all redress requests that comes to CBP directly, and concerns 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 created a comprehensive Department-wide program, called the Traveler Redress Inquiry Program (DHS TRIP), to receive all traveler-related comments, complaints, and redress requests affecting its component agencies. Through DHS TRIP, travelers can seek resolution regarding difficulties they experienced during their travel screening and inspection.[61]

Under the ATS PIA and SORN, and as a matter of DHS policy,[62] CBP permits subjects of PNR or their representatives to make administrative requests for access and amendments 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 provided for access in the source systems for ingested data, so that individuals may request access to their own data from either ATS (if ATS is the source system) 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), the Privacy Act, and the Judicial Redress Act (JRA) provide additional means of access to PII held in source systems.[63] FOIA, Privacy Act, and JRA requests for access to information for which ATS is the source system are directed to CBP.[64]

---

[59] 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.

[60] The Pledge is available at https://www.cbp.gov/travel/customer-service/cbp-pledge-to-travelers. In addition, travelers can visit CBP's INFO Center website at https://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.

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

[62] https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

[63] 5 U.S.C. § 552; 5 U.S.C. § 552a; 5a; 5 U.S.C. § 552a note.

[64] Requests may be submitted electronically to CBP's FOIA Officer by visiting: https://foiaonline.gov/foiaonline/action/public/home or mailed to FOIA Officer, U.S. Customs and Border Protection, 90 K Street, NE, FOIA Division, Washington, DC 20229.

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 Professional Responsibility 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, except as noted below.[65] The retention period for PNR, which is contained only in ATS-P, is subject to the following further access restrictions and masking requirements: ATS-P users with PNR access have access to PNR in an active status 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 status, the PNR is transferred to a dormant status 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 an appropriate CBP supervisor. Furthermore, PNR in the dormant status may only be unmasked in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk.[66]

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.

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

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

## B. Analytical Framework for Intelligence (AFI)

In August 2020, the AFI PIA was updated to permit access to AFI by additional DHS components including the DHS Office of Inspector General (OIG).[67]

### 1. 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. It also 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, identifying cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law; (2) conducting additional research on persons or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and (3) sharing finished intelligence products[68] 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 CBP Intelligence Records System (CIRS) SORN.[69]

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 analysts use AFI to conduct research on individuals, cargo, or conveyances to assist in identifying potential law enforcement or security risks. AFI simply 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 allow analysts to search several data bases simultaneously and provides a set of analytical tools that includes advanced search capabilities into existing DHS data sources, and federated queries to other federal agency sources and commercial data aggregators. AFI tools present the results to the AFI analyst in a manner that allows for easy visualization and analysis.

---

[67] The PIA for AFI is available at: http://www.dhs.gov/privacy-impact-assessments.

[68] "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.

[69] DHS/CBP-024 Intelligence Records System (CIRS) System of Records, (September 21, 2017) 82 FR 44198.

AFI enables 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. AFI creates an index of the relevant data in existing operational DHS sources systems by ingesting this data source data systems, as describe below, to enable faster return of search results. 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. Finished intelligence products and unfinished "projects"[70] are also part of the index.

With other systems, a search for an individual requires several queries across multiple systems to retrieve a corresponding response and may not contain all relevant instances of the search terms. 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 an individual or characteristic arises.

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 products, and to share finished intelligence products either within DHS based on a need to know or externally through regular law enforcement and intelligence channels to authorized users pursuant to routine uses described in the CIRS SORN.[71]

### 2. 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.

[70] 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.

[71] DHS/CBP-024 Intelligence Records System (CIRS) System of Records, (September 21, 2017) 82 FR 44198. A detailed description of the processes leading to finished intelligence products and RFI responses is included in the PIA for AFI *available at* https://www.dhs.gov/privacy.

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

Specific types of analysis include:

- *Geospatial analysis*: Geospatial analysis utilizes visualization tools to display a set of events or activities on a map showing streets, buildings, geopolitical borders, or terrain. This analysis can help produce intelligence about the location or type of location that is favorable for a particular activity.
- *Link analysis*: Link analysis provides visualization tools that can help analysts discover patterns of associations among various entities.
- *Temporal analysis*: Temporal analysis offers visualization tools that can display events or activities in a timeline to help the analyst identify patterns or associations in the data. This analysis can produce a time sequence of events.

The results of these analyses are used to generate finished intelligence products and projects. The finished intelligence products are published in AFI for finished intelligence products users to search. In all situations, research developed by or reports created by AFI analysts are subject to supervisory review.

### 3. Data Sources

The AFI system does not 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 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[72]:

- *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);

[72] AFI has published Appendix B that lists all of the data sources that are available through AFI. Appendix B can be found at: https://www.dhs.gov/publication/analytical-framework-intelligence-afi.

- Select legacy IFS datasets (including the following information: EID detention data,[73] ICE intelligence information reports, ICE intelligence products, ICE name trace, ICE significant event notification, Detention and Removal Leads, and TECS Reports of Investigation).[74]
- Enterprise Management Information System-Enterprise Data Warehouse (including: Arrival and Departure Form I-94[75]; CMIR data;[76] apprehension, inadmissibility, and seizure information from the ICE Criminal Arrest Records and Immigration Enforcement Records (CARIER);[77] National Security Entry-Exit Program information from CARIER; SEVIS information;[78] and seizure information from the Seized Asset and Case Tracking System[79]); 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.[80]
- *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-provide information that 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.

---

[73] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at:* https://www.dhs.gov/privacy.
[74] *See* DHS/ICE/PIA-007 Law Enforcement Intelligence Fusion System (IFS), *available at* https://www.dhs.gov/privacy.
[75] *See* DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS) *available at* https://www.dhs.gov/privacy.
[76] The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.
[77] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), (Oct. 19, 2016) 81 Fed. Reg. 72080.
[78] *See* DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) *available at* https://www.dhs.gov/privacy. DHS/ICE-001 Student and Exchange Visitor Information System, (Jan. 5, 2010) 75 Fed. Reg. 412.
[79] DHS/CBP-013 Seized Assets and Case Tracking System, (Dec. 19, 2008) 73 Fed. Reg. 77764.
[80] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates ATS PIA *available at* https://www.dhs.gov/privacy for a more complete discussion of other government agency data that may be accessed through ATS.

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 the appropriate user groups.
- *Index Information*: As noted above, AFI ingests subsets of data from CBP and DHS systems to create an index of searchable data elements. The index indicates which source system records match the search term used.

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

### 4. Efficacy

AFI became operational in August 2012, and since that time, 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. Continued operational use of AFI provides improved information sharing amongst participating DHS components. CBP personnel were able to use AFI's search capabilities to identify connections between previously uncorrelated human smuggling events. This allowed CBP to associate individuals to multiple smuggling events and deliver greater insight into the criminal organization behind the activities. CBP officers were able to use AFI's batch search capabilities to search for several hundred entities (individuals and locations) across multiple CBP data sources much faster than they could without AFI. This provided the officers more time to review the responsive records and take appropriate action. In 2019, AFI enabled the identification of previously unknown connections in a narcotics case through its link analysis capability, better assessment of interview data to identify and compare trends using AFI's search function and identifying a subject of interest in a minor trafficking case through the ability to combine multiple incomplete selectors.

### 5. 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 *Implementing Recommendations of the 9/11 Commission Act of 2007* (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.

### 6. Privacy Impact and Privacy Protections

CBP has built extensive privacy protections into the structure and governance of AFI.[81] AFI itself does not collect information directly from individuals and CBP does not use the information in AFI

[81] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) *available at* http://https://www.dhs.gov/privacy.

to make unevaluated automated decision about individuals. AFI source systems are responsible for providing individuals the opportunity to consent to, opt-out of, or decline to provide information or the use of their information, as appropriate. AFI provides the public notice about its use of information through its PIA and CIRS SORN.[82]

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 and Marine, Chief Counsel, Internal Affairs, Information Technology, and Privacy and Diversity. The board members review requested changes to the system on a quarterly basis and determine whether additional input is required. They also evaluate the need for developing enhancements to AFI, review and approve new uses to the system for new or updated user types, as well as new or expanded data capabilities. As an added layer of oversight, the DHS Privacy Office conducted and published Privacy Compliance Reviews (PCRs) for AFI on December 19, 2014[83] and December 6, 2016.[84]

Although AFI indexes information from many different source data systems, each source system maintains control of the data that it originally collected, even though the data is also maintained in AFI. Accordingly, only DHS AFI analysts authorized to access the data in a source system have access to that same data through AFI.[85] This is accomplished by passing individual user credentials from the originating system or through a previously approved certification process in another system. Finished intelligence products 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. To access AFI, all AFI users are required to complete annual training in privacy awareness. All CBP employees are required to have the required privacy training in order to access law enforcement systems. This training is updated regularly and users who do not complete this training lose access and privileges to all CBP computer systems, including AFI.

AFI does not collect information directly from the public or any other primary source. Therefore, data accuracy is dependent upon the system(s) performing the original collection. 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 depends 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 any inaccuracies and alert the source agency of the inaccuracy. AFI will then reflect the corrected information. Additionally, as the source systems for other federal

[82] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) *available at* http://https://www.dhs.gov/privacy. DHS/CBP-024 Intelligence Records System (CIRS) System of Records, (September 21, 2017) 82 FR 44198.
[83] The 2014 AFI PCR is available at: https://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.
[84] The 2016 AFI PCR is available at: https://www.dhs.gov/sites/default/files/publications/AFI%20PCR%20final%2012062016.pdf.
[85] Only authorized CBP personnel and analysts who require access to the functionality and data in AFI as a part of the performance of their official duties and who have appropriate clearances or permissions will have access to AFI.

agency data or commercial data aggregators correct information, queries of those systems will reflect the corrected information.

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 is available to its users. Any changes to the source system record, 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 users can 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 is 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 a 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). In April 2017, AFI was granted an ongoing authority to operate (OATO) 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, law enforcement programs, activities, and investigations, DHS has exempted AFI from the access and amendment provisions of the *Privacy Act*, 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 are no exemptions for giving access to a record in a source system, CBP will provide access to that information maintained in AFI.[86]

To the extent that CBP accesses and incorporates information from other DHS systems of records as sources of information for finished intelligence products, CBP will abide by the safeguards, retention schedules, and dissemination requirements of those underlying source systems of record.

[86] 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. Additional information on submitting FOIA and Privacy Act requests is included in the PIA. *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) *available at*: https://www.dhs.gov/privacy.

Consistent with the *DHS N1-563-07-016* records schedule (May 30, 2008), CBP will retain information consistent with the same retention requirements of the DHS Office of Intelligence and Analysis:

1. Dissemination Files and Lists: CBP will retain finished and current intelligence report information distributed to support the Intelligence Community, DHS Components, and federal, state, local, tribal, and foreign Governments and includes contact information for the distribution of finished and current intelligence reports for two (2) years.

2. Raw Reporting Files: CBP will retain raw, unevaluated information on threat reporting originating from operational data and supporting documentation that are not covered by an existing DHS system of records for thirty (30) years.

3. Finished Intelligence Case Files: CBP will retain finished intelligence and associated background material for products such as Warning Products identifying imminent homeland security threats, Assessments providing intelligence analysis on specific topics, executive products providing intelligence reporting to senior leadership, intelligence summaries about current intelligence events, and periodic reports containing intelligence awareness information for specific region, sector, or subject/area of interest as permanent records and will transfer the records to the NARA after twenty (20) years.

4. Requests for Information/Data Calls: CBP will retain requests for information and corresponding research, responses, and supporting documentation for ten (10) years.

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

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

ICE published the FALCON-DARTTS PIA on January 16, 2014[88] and updated and published the FALCON Search & Analysis (FALCON-SA) Appendix to reflect that specific datasets and analytical results from FALCON-DARTTS are ingested into FALCON-SA.[89] On December 1, 2014, ICE republished the Trade Transparency Analysis and Research (TTAR) SORN, which

[87] In February 2012, ICE deployed the first module of FALCON with the launch of FALCON Search & Analysis (FALCON-SA. FALCON-SA provides the capability to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. For more information on the FALCON environment. *See* DHS/ICE/PIA-032A FALCON Search & Analysis System (FALCON-SA) *available at* https://www.dhs.gov/privacy.

[88] *See* DHS/ICE/PIA-038 FALCON Data Analysis & research for Trade Transparency System (FALCON-DARTTS), *available at* https://www.dhs.gov/privacy.
https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falcondartts_january2014_0.pdf.

[89] *See* DHS/ICE/PIA-032(a) FALCON Search & Analysis System (FALCON-SA), *available at* http://https://www.dhs.gov/privacy.

applies to FALCON-DARTTS.[90]

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

### 1. Program Description

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

FALCON-DARTTS is owned and operated by the HSI Trade Transparency Unit (TTU). Trade transparency is the examination of U.S. and foreign trade data to identify anomalies in patterns of trade. Such anomalies may 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. Pursuant to their mission, 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 breadth of data it accesses and the number and type of variables through which it can sort.[91] FALCON-DARTTS does not seek to predict future behavior or "profile" individuals or entities (i.e., identify individuals or entities that meet a certain pattern of behavior pre-determined to be suspect). Instead, it identifies trade and financial transactions that are statistically anomalous based on user-specified queries. Investigators further examine the anomalous transactions to determine if they are, in fact, suspicious and warrant further investigation. HSI special agents 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

[90] *See* DHS/ICE-005, Trade Transparency Analysis and Research (TTAR), (Dec. 1, 2014) 79 Fed. Reg. 71112. Datasets analyzed by FALCON-DARTTS not listed in the TTAR SORN at the time the system became operational in January 2014 were restricted from use in the system until the effective date of the updated SORN published in the *Federal Register*.

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

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, may also use specific trade datasets to investigate trade transactions, conduct analysis, and generate reports in FALCON-DARTTS.

FALCON-DARTTS uses trade data, financial data, and law enforcement data provided by other U.S. government agencies and foreign governments (hereafter referred to collectively as "raw data"). 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. Financial data includes the following PII: names of individuals engaging in financial transactions that are required to be reported pursuant to 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. Financial data consists of financial transaction reports filed pursuant to the BSA provided by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and other financial data provided to HSI by federal, state, and local law enforcement agencies. Law enforcement data consists of the publicly available Specially Designated Nationals (SDN) List compiled and maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), as well as subject records from CBP TECS. All ICE HSI, CBP, and foreign users of FALCON-DARTTS can only access data that is associated with the user's specific profile and which that user has the legal authority to access. Specifically, only ICE HSI and CBP users are granted access to the law enforcement data, and only ICE HSI users are granted access to the financial data maintained in FALCON's general data storage environment.[92] In this environment, the data is aggregated with other FALCON data, and user access is controlled through a combination of data tagging, access control lists, and other technologies.

Through existing CMAAs and Memorandum of Understanding (MOUs), ICE HSI exchanges International Currency and Monetary Reports (FinCEN Form 105) on a reciprocal basis with three countries: Colombia, Mexico, and France. Except for these three countries, foreign users of FALCON-DARTTS are authorized to access only trade data, and are not authorized to access the law enforcement, financial data, or any *ad hoc* data that may reside 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

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

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 can access only the trade data about individuals or institutions with status in their country and the related U.S. trade transactions unless access to other partner countries' data is authorized via information sharing agreements with DHS.

### 2. Technology and Methodology

FALCON-DARTTS uses COTS software to assist its users in identifying suspicious trade transactions by analyzing trade and financial data and identifying data that is statistically anomalous. In response to user-specified queries, the software application is designed to analyze structured and unstructured data using three tools: the drill-down technique,[93] link analysis, and charting and graphing tools that use proprietary statistical algorithms.[94] It also allows non-technical users with investigative experience to analyze large quantities of data and rapidly identify problem areas. Through its sorting capability, the program facilitates application of specific knowledge and expertise to complex sets of data.

FALCON-DARTTS performs three main types of analysis. First, 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. Second, 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. Third, it 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 or addresses. 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 receives data from the sources discussed below via CD-ROM, external storage devices, or electronic data transfers. The agencies that provide FALCON-DARTTS with trade data collect any PII directly from individuals or enterprises completing import-export electronic or paper

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

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

forms.[95] 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.[96] PII contained in the raw data is necessary to link related transactions together. It is also necessary to identify persons or entities that should be investigated further.

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

### 3. 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

[95] 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.

[96] 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.

States who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via ACS; (2) EEI submitted to AES; and (3) bill of lading data collected by CBP via the AMS and provided to ICE through electronic data transfers for upload into FALCON-DARTTS.

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

ICE may receive U.S. financial data from FinCEN or federal, state, and local law enforcement agencies. BSA data is in the form of the following financial transaction reports: CMIRs (transportation of more than $10,000 into or out of the United States at one time); Currency Transaction Reports (deposits or withdrawals of more than $10,000 in currency into or from a domestic financial institution); Suspicious Activity Reports (information regarding suspicious financial transactions within depository institutions, money services businesses,[97] 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.[98]

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

Subject records created by ICE HSI users from CBP's TECS database pertain to persons, vehicles, vessels, businesses, aircraft, etc. FALCON-DARTTS accesses this data stored within the FALCON

[97] The BSA, pursuant to 31 U.S.C. § 5318, requires a money services business (MSB) 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.

[98] 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.

general data storage environment, eliminating the need for an additional copy of the data. FALCON-DARTTS analysis of TECS subject records allows ICE HSI users to determine quickly if an entity that is being researched in FALCON-DARTTS is already part of a pending investigation or was involved in an investigation that is now closed.

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

### 4. Efficacy

Through the use of FALCON-DARTTS, domestic HSI field offices and foreign attaché offices have the ability to initiate and enhance criminal investigations related to trade-based money laundering, trade fraud, and other financial crimes.

The FALCON-DARTTS system has been instrumental as an investigative tool in numerous HSI criminal investigations. While in FY2019 there have been no major success stories, past performance indicates that the tool will continue to be effective moving forward.

### 5. 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 pursuant to *18 U.S.C. §§ 541, 542, 545, and 554*; money laundering investigations pursuant to *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*,[99] the *Trade Secrets Act*,[100] and *BSA*.[101]

### 6. Privacy Impact and Privacy Protections

ICE does not use FALCON-DARTTS to make unevaluated decisions about individuals; FALCON-

[99] 5 U.S.C. § 552a.
[100] 18 U.S.C. § 1905.
[101] 31 U.S.C. § 5311.

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 amendment requests under the Privacy Act, and access or amendment is granted 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.[102] FALCON-DARTTS will coordinate requests for access or requests 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.[103]

All raw data analyzed by FALCON-DARTTS is obtained from other governmental organizations that collect the data under specific statutory authority. Therefore, FALCON-DARTTS relies on the systems and/or programs performing the original collection to provide accurate data. Most of the raw data used by FALCON-DARTTS is presumed accurate because the data was collected directly from the individual or entity to whom the data pertains. Due to the law enforcement context in which FALCON-DARTTS is used, however, there are often significant impediments to directly verifying the accuracy of information with the individual to whom the specific information pertains.[104] 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

[102] The following SORNs published in the Federal Register 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) (79 Fed. Reg. 20969 (April 14, 2014), *available at:* https://www.federalregister.gov/documents/2014/04/14/2014-08254/privacy-act-of-1974-as-amended-system-of-records-notice); and for CBP Information, DHS/CBP-001, Import Information System, 81 Fed. Reg. 48826 (July 26, 2016), *available at:* https://www.regulations.gov/document?D=DHS-2016-0048-0001; ACS, DHS/CBP-015, 73 Fed. Reg. 77759 (Dec. 19, 2008), *available at:* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29801.htm; and TECS, DHS/CBP-011, 73 Fed. Reg. 77778 (Dec. 19, 2008), *available at:* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm).

[103] DHS/ICE-005 Trade Transparency Analysis and Research (TTAR), (December 1, 2014) 79 FR 71112.

[104] 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.

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 is 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 then used to identify users who are using the system improperly.[105]
In addition to the auditing and accountability functions leveraged from FALCON-SA, FALCON-DARTTS maintains additional audit trail functionality derived from the July 2006 MOU with the U.S. Department of the Treasury's FinCEN. In that agreement, FALCON-DARTTS was to track, for each query, the identity of the user, time and nature of the query, as well as the BSA information viewed.

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

In 2009, NARA approved a record retention period for information maintained in the legacy DARTTS system.[106] ICE had intended to request NARA approval to retire the legacy DARTTS records retention schedule and incorporate retention periods for data accessible by FALCON-DARTTS into a records schedule for the FALCON environment. However, this effort was stopped as ICE no longer creates system record schedules. There is an ongoing effort to draft an ICE records schedule for investigative records. This includes information maintained in DARTTS. There is no current timeframe for completion of this records schedule. Until it is completed, the datasets used by FALCON-DARTTS will be retained for ten years per the above-mentioned legacy DARTTS

[105] For more information on these controls, auditing, and accountability, *See* DHS/ICE/PIA-032(a) FALCON Search & Analysis System (FALCON-SA), *available at* http://https://www.dhs.gov/privacy.
[106] *See* N1-567-09-3 (Nov. 9, 2009).

records schedule. Some of the data used by FALCON-DARTTS is already maintained in the FALCON general data storage environment and subject to a proposed retention period; however, FALCON-DARTTS will only access these existing datasets for ten years. Several new datasets were added to the FALCON general storage environment with the launch of FALCON-DARTTS, and the retention and access period for those datasets is proposed to be ten years as well.

### D. FALCON-Roadrunner

FALCON-Roadrunner ceased operation in the beginning of FY 2018. During the FY 2019 reporting period, ICE completed data migration of the data used for FALCON-Roadrunner from the FALCON data storage environment into the Repository for Analytics in a Virtualized Environment (RAVEn). RAVEn is not currently using any data for data mining purposes.

ICE is currently drafting a Disposition Privacy Threshold Analysis to reflect that the FALCON-Roadrunner system is no longer in operation. This will memorialize that ICE no longer uses the system, including for data mining purposes.

### E. SOCRATES

During the reporting period, CBP finalized the last contract with Johns Hopkins University for the SOCRATES pilot. CBP's Trade Remedy Law Enforcement Directorate (TRLED), within the Office of International Trade (OT), worked 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),[107] 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 which analytical abilities JHU/APL could apply to trade data analytics. In October 2019, the SOCRATES pilot was decommissioned and never became an operational program. A SOCRATES PTA was completed however no further compliance documentation was pursued when the program was decommissioned.

JHU/APL used a government-off-the-shelf product named SOCRATES, developed by mathematicians at JHU/APL. SOCRATES, in conjunction with supporting software, was used to develop algorithms to analyze large datasets looking for both normal and abnormal trade patterns of behavior. This resulted 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.

[107] 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.

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 was extracted from ATS[108] and ACE[109] on a monthly basis. The data pulled from ATS consisted only of cargo examination data contained in the Cargo Enforcement Reporting and Tracking System (CERTS) portion of ATS. ACE data included entry summary transactions filed with CBP by importers for the last 10 years of transaction data. This data contained 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).[110] SOCRATES did not interact directly with CBP's systems. SOCRATES was housed on CBP servers connected to CBP's network. Only CBP-cleared JHU/APL team members that signed a non-disclosure agreement, had a CBP Personal Identity Verification card, and CBP network access could work on SOCRATES and CBP Trade Data. User activity was logged by the CBP Office of Information and Technology (OIT) and by the CBP server housing SOCRATES.

Validation of results during the pilot included CBP analysts or CBP subject matter experts reviewing and determining whether the analytic results compared similarly to past CBP findings or provided additional recommendations for further review. Additional review of the analytics selections and in-depth determinations were conducted for results outside of past CBP findings. CBP will take lessons learned about analytics from this pilot and apply it to programs that are in development.

The legal authorities for CBP's SOCRATES pilot included: *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*.

### F. Fraud Detection and National Security – Data System (FDNS-DS)/ATLAS

During the reporting period, USCIS enhanced screening capabilities to include additions to Continuous Immigration Vetting (CIV) updates within the ATLAS system. CIV is an event-based vetting tool that automates and streamlines the process of notifying USCIS of potential derogatory information in government databases that may relate to individuals in USCIS systems, as new information is discovered. USCIS published a CIV PIA in December 2018 to address CIV privacy capabilities and privacy concerns.

ATLAS continues to serve as a conduit to facilitate screening of applications, petitions and other immigration-related requests. ATLAS promotes consistent identification and analysis of fraud, public safety, and national security concerns with immigration requests and automates the referral

[108] 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.
[109] 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.
[110] 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.

of potential concerns to the USCIS Fraud Detection and National Security Directorate (FDNS) for review and administrative investigation. The content for this report has been updated to reflect current ATLAS screening metrics for the reporting period.

### 1. Program Description

Every year, USCIS receives nearly 9.5 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' 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 Data System (FDNS-DS)[111] to record, track, and manage cases 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 developed a platform called 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' screening capability enhances the integrity of the immigration process and strengthens USCIS' obligations of the Immigration and Nationality Act (INA) through the following benefits:

i. SGNs preemptively notify FDNS Officers of suspected fraudulent or nefarious information before adjudicators begin reviewing applications and provides updates on existing applicant filings through continuous vetting and monitoring;

ii. Increases consistency and timeliness for background and security check operations;

iii. Ensures consistent process and procedures to operationalize screening enhancements; and

iv. Integrates screening capabilities with USCIS case management systems.

### 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

[111] *See* DHS/USCIS/PIA-013 Fraud Detection and National Security Data System (FDNS-DS), *available at* https://www.dhs.gov/privacy. DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) (Aug. 8, 2012) 77 Fed. Reg. 47411.

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' IDENT Fingerprint Check[112], and Department of Defense Automated Biometric Identification System (ABIS) Fingerprint Check[113]; and biographic, name-based checks such as the FBI Name Check and TECS[114] 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 promotes consistent identification, storage, retrieval, and analysis of screening results to enable FDNS to more efficiently and effectively detect and investigate fraud, public safety, and national security concerns.

ATLAS' automated, event-based screening is triggered when:

A. An individual presents him or herself to the agency (i.e., when USCIS receives an individual's application, such as for adjustment of status; when there is an update to an application; or when an applicant's fingerprints are taken at an authorized biometric capture site as part of the form application process); or

B. Derogatory information is associated with the individual in one or more DHS systems.

ATLAS receives information from the individual's form submission and from the biographic and biometric-based checks listed above. This information is screened through ATLAS' rules engine, producing SGNs to automate the process of referring cases to FDNS for review. A specially trained FDNS Officer, known as a Gatekeeper, conducts a manual review of the SGN for validity, and 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 more efficiently identify discrepancies.

[112] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at*: https://www.dhs.gov/privacy.

[113] 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*: https://www.dhs.gov/privacy.

[114] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at*: https://www.dhs.gov/privacy.

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 produce findings to inform adjudications.

ATLAS allows for easier identification of individuals who are filing for immigration and naturalization benefits who may potentially be engaging in fraudulent behavior or who may pose a risk to public safety or national security. During the screening process, ATLAS analyzes the results of biographic and biometric checks, and applies rules against data received from multiple systems. ATLAS assists in confirming individuals' identities in stances where individuals are potentially known by more than one identity. This confirmation is done by comparing the identity information provided by the individual against identity information resident in other systems used with the security verification process. For example, ATLAS can determine if an individual has applied for benefits using multiple biographic identities or aliases by matching fingerprints for the various identities. The results of this analysis may be produced and sent to FDNS-DS in the form of an SGN.

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

### 3. Data Sources

SGNs pushed into FDNS-DS contain information collected from various systems and culled based on the specific rule criteria for each SGN. Below is a list of systems, both internal and external, that pass applicant biographic information (including biographic data from an application or associated with a biometric capture) through ATLAS to fulfill screening requirements. Any rule-based detection of potential derogatory information will result in an SGN within FDNS-DS.

*U.S. Citizenship and Immigration Services (USCIS) Systems*: National Benefit Center Process Workflow Repository (NPWR)[115] to facilitate screening for CAMINO[116] and certain form types being processed through the National Benefit Center and Service Center Operations; Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR)[117]; USCIS Electronic Immigration System (ELIS)[118]; TECS by ELIS [119] to facilitate checks by Computer Linked Application Information Management System (CLAIMS 3)[120]; GLOBAL[121];RAILS[122] to

[115] NPWR is covered under DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization (CLAIMS 3), *available at* https://www.dhs.gov/privacy.
[116] *See* DHS/USCIS/PIA-051 CAMINO, *available at:* https://www.dhs.gov/privacy.
[117] *See* DHS/USCIS/PIA-023(a) eCISCOR, *available at* https://www.dhs.gov/privacy.
[118] The DHS/USCIS/PIA-056 USCIS ELIS PIA is *available at:* http://www.dhs.gov/privacy.
[119] See DHS/USCIS/PIA-056 (d) USCIS Electronic Immigration System (USCIS ELIS) is available at: http://www.dhs.gov/privacy.
[120] The DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems PIAs are available at: http://www.dhs.gov/privacy.
[121] *See* DHS/USCIS-027(c) Asylum Division, *available at:* http://www.dhs.gov/privacy.
[122] The DHS/USCIS/PIA-032 National File Tracking System (NFTS) PIA is available at http://www.dhs.gov/privacy.

retrieve the physical locations of A-files; and, Customer Profile Management System (CPMS)[123] to retrieve data associated with biographic and biometric screening.

*Other U.S. Department of Homeland Security (DHS) Component System Interfaces*: IDENT[124] to retrieve data associated with biometric screening; CBP's TECS[125] system, system via the CBP TECS Screening Service (TSSV)platform, to perform screening, including checks against the FBI, National Crime Information Center (NCIC); ATS-P[126] and UPAX; and DHS Email as a Service (EaaS) Simple Mail Transfer Protocol (SMTP)[127] 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;[128] ADIS;[129] SEVIS;[130] and ENFORCE[131]Alien Removal Module:

*External Sources Accessed (Manually)*: Department of Labor; DoS; Department of Defense; 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.

### 4. Efficacy

The 2020-2024 DHS Strategic Plan states that, "DHS is more thoroughly screening and vetting individuals seeking immigration benefits and seeking entry to the United States, ensuring immigration benefits comport with legislative intent and emphasize American economic needs, and eliminating opportunities for systematic abuse of the U.S. immigration system at the expense of the American people."[132] ATLAS is a platform that enhances the ability of USCIS to detect and investigate fraud, national security and public safety concerns, in forms submitted to USCIS.

---

[123] The DHS/USCIS/PIA-060 Customer Profile Management Service PIA is available at: http://www.dhs.gov/privacy.
[124] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at*: https://www.dhs.gov/privacy.
[125] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at*: https://www.dhs.gov/privacy.
[126] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at*: https://www.dhs.gov/privacy.
[127] *See* DHS/ALL/PIA-012 E-mail Secure Gateway and subsequent updates, *available at*: https://www.dhs.gov/privacy.
[128] *See* DHS/CBP/PIA-010 AFI, *available at*: https://www.dhs.gov/privacy.
[129] *See* DHS/CBP/PIA-24 Arrival and Departure Information System (ADIS), *available at*: https://www.dhs.gov/privacy.
[130] *See* DHS/ICE/PIA-001(b) Student and Exchange Visitor Information System II (SEVIS), *available at*: https://www.dhs.gov/privacy.
[131] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at*: https://www.dhs.gov/privacy.
[132] U.S. Department of Homeland Security. "Fiscal Years 2020 – 2024 Strategic Plan," available at: https://www.dhs.gov/publication/department-homeland-securitys-strategic-plan-fiscal-years-2020-2024, page 24.

ATLAS is capable of screening biometric and biographic information associated with forms submitted to USCIS automatically at intake, resolving identities when individuals use aliases.

In Fiscal Year 2019, ATLAS screened over 48 million biographic checks on more than 9.5 million unique application filings, and over 7 million biometric screenings against IDENT biometric repository, resulting in more than 123,000 SGNs created. SGNs generated in Fiscal Year 2019 resulted in 4,441 new immigration benefit fraud concerns, 734 new public safety concerns, and 480 national security concerns.[133]

ATLAS alerts FDNS Officers to potential concerns much earlier in the immigration process. USCIS has achieved efficiencies and successes with the deployment of ATLAS, rather than continuing to rely on multiple manual, point-in-time checks, to identify potential derogatory matches within DHS vetting systems as new information is discovered. For instance, on March 17, 2018, ATLAS created a Continuous Immigration Vetting (CIV) SGN for an N-400 applicant. The applicant submitted the application on February 16, 2018. Initial screening conducted on February 17, 2018 was negative. After the applicant provided biometrics and the information was ingested into IDENT, an additional alias was identified by ATLAS and pulled into CIV. Derogatory information was detected outside of regular point-in-time checks under a slight variation of the subject's name for information valuable to the adjudicative process.

In another instance, a USCIS officer triaged an SGN on February 12, 2019 relating to multiple identities fraud. It was found the naturalized individual had adjusted to lawful permanent resident status and naturalized using a false identity. The use of multiple identities was confirmed through a match to a single Fingerprint Identification Number as well as an executed Final Removal Order (FRO) issued by an immigration judge. The FDNS review found the individual had been detained on June 17, 1992 on the charge of No Valid Immigration Visa and ordered deported on November 29, 1993 under one identity. Later, the subject adjusted status and naturalized under another identity, failing to disclose use of multiple identities and deportation. The fraud and misrepresentation made by subject closed off a material line of inquiry. Had USCIS been made aware of the subject's derogatory information history and use of multiple identities, he would not have obtained U.S. Citizenship. USCIS determined fraud was found and presented the case to USCIS Office of the Chief Counsel, who accepted and submitted to the DOJ Civil Denaturalization. The DOJ, Office of Immigration Litigation (OIL) has accepted the case and the individual will be processed for administrative denaturalization in federal court.

### 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. This includes discovering incidents of immigration fraud and ensuring that individuals who pose national security threats are not granted immigration benefits. The DHS Secretary 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

[133] FY 2019 data compiled from Fraud Detection and National Security Data System (FDNS-DS) data as of October 3, 2019.

section *101(a)(17) of the INA*); and (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 Bureau of Citizenship and Immigration Services [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.[134] 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[135] 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,'[136] or has engaged in or is suspected of engaging in terrorist activities.[137] Similarly, *section 237* of the INA[138] 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[139] or security and related grounds.[140]

### 6. Privacy Impact and Privacy Protections

FDNS is focused on effective identification of threats to national security and public safety, detection and combating immigration benefit fraud, and removal of systematic and other vulnerabilities, respecting individuals' privacy and promoting transparency of FDNS operations. In May 2016, FDNS updated and re-issued its PIA for the FDNS-DS system[141] 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.

FDNS has a vested interest and responsibility to maintain the most accurate data possible since the information it collects could be used in support of an adjudicative decision or criminal investigations undertaken by law enforcement partners. FDNS Officers rely on multiple sources to confirm the veracity of data and, if discrepancies are uncovered, take the necessary steps to correct inaccuracies. This confirmation includes 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 data integrity. In the event FDNS Officers learn information contained within other

[134] INA § 245(a)(2), 8 U.S.C. § 1255, ("Adjustment of status of non-immigrant to that of person admitted for permanent residence").
[135] *Id*. at § 212. 8 U.S.C. § 1255 ("Inadmissible aliens").
[136] *Id*. at § 212(a)(2), 8 U.S.C. § 1182(a)(2) ("Criminal and related grounds").
[137] *Id*. at § 212(a)(3), 8 U.S.C. § 1182(a)(3) ("Security and related grounds").
[138] *Id*. at § 237, 8 U.S.C. § 1227 ("General classes of deportable aliens").
[139] *Id*. at § 237(a)(2), 8 U.S.C. §1227(a)(2) ("Criminal offense").
[140] *Id*. at § 237(a)(4), 8 U.S.C. §1227(a)(4) ("Security and related grounds").
[141] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* https://www.dhs.gov/privacy.

systems is not accurate, the Officer will notify appropriate USCIS personnel or the federal agency owning the data, who will facilitate 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 C.F.R. § 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 may 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' rules-based screening approach is tailored to provide information to FDNS Officers relevant to potential fraud, public safety, and national security threats. 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.
Multiple layers of privacy and legal review are built into FDNS' processes, to reduce the risk of new data being incorporated into FDNS that has not been reviewed for privacy and legal concerns. Additionally, FDNS must submit a PTA and receive approval from the DHS Privacy Office before adding any new data sources.

Since FDNS-DS contains sensitive PII, related to possible immigration benefit fraud and national security concerns, DHS has exempted FDNS from the 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.

### G. Global Command and Control System - Joint

#### 1. Program Description

The Global Command and Control System – Joint (GCCS-J) is the Department of Defense's (DoD) command and control (C2) system of record, implemented as the foundation of the United States Coast Guard's (USCG) classified C2 system. The Defense Information Systems Agency (DISA) developed GCCS-J and the USCG uses it to subscribe and publish to other USCG and DoD classified C2 systems, as well as to subscribe to USCG's Unclassified Common Operating Picture (UCOP), in order to supplement the USCG's classified COP.

GCCS-J provides decision makers with a detailed view of their respective Area of Responsibility on both a strategic and tactical level. This includes current locations, planned movements, and all available status information for friendly, neutral, and enemy ground, maritime, and air units. GCCS-J also displays all available information that can enhance Maritime Domain Awareness (MDA).

More information addressing the Law Enforcement Sensitive aspects of this program are being provided in an annex to the report.

#### 2. Technology and Methodology

GCCS-J is a Commercial of the Shelf (COTS) product specifically built to perform a detailed view of a respective Area of Responsibility (AOR) on both a strategic and tactical level.

#### 3. Data Sources

On an operator to operator basis, GCCS-J data sources are used for tracking of locations. In addition, data from the National Oceanic and Atmospheric Administration's (NOAA) Vessel Monitoring System database provides near real time positional information.

#### 4. Efficacy

GCCS-J enables Operators and Intelligence Analysts to more effectively schedule limited government resources to identify, and if necessary, interdict or intervene when required. It is a critical component of the Common Operational Picture (COP) and provides decision makers a detailed view of their respective AOR either on a strategic or tactical level. This visibility includes current locations, planned movements and all available status information for friendly, neutral, and enemy ground, maritime, and air units.

Additionally, GCCS-J displays available information that could impact the disposition of friendly, neutral, and enemy ground, maritime, and air units (e.g., weather). System overlays depicting zones and areas are arrayed in a manner to assist decision makers in assessing current conditions thereby further enhancing their Maritime Domain Awareness (MDA).

### 5. Laws and Regulations

Certain laws and regulations apply to the data used in GCCS-J and apply to protect individuals' privacy and due process rights in connection with *GCCS-J. USCG Cybersecurity Manual, COMDTINST M5500.13* series and *Classified Information Management Program, COMDTINST M5510.23* apply to the data used in GCCS-J.

### 6. Privacy Impact and Privacy Protections

USCG use of GCCS-J is granted through a MOU between USCG and the Department of Defense's United States Strategic Command for GCCS-J, dated March 23, 2019. This MOU implemented the use of GCCS-J by providing roles, responsibilities, ownership, and accountability in the use of the system. In addition, USCG entered into a separate MOU on May 7, 2018, that allowed USCG to inherit DISA's Authority to Operate for use by USCG.

In 2019, GCCS-J underwent a PTA to assess whether there is a need for additional Privacy compliance documentation; a determination was made that the PTA was sufficient.

## H. U.S Coast Guard Unclassified Common Operating Picture (UCOP)

### 1. Program Description

The USCG's UCOP consumes and disseminates unclassified products that aid MDA, subsequent decision-making, and Command and Control. UCOP aggregates unclassified data reports from land, maritime, air, and interagency USCG-controlled assets, including data feeds from asset sensors, intelligence sources, and DoD agencies. UCOP provides unclassified raw (uncorrelated) and correlated products to unclassified and classified systems and their users. In addition to being the USCG's authoritative source for unclassified track data, UCOP provides unclassified data to augment the classified COP.

NOAA's Vessel Monitoring System (VMS) allows the USCG Office of Law Enforcement (OLE) to monitor and survey vessels over vast expanses of open water while maintaining the confidentiality of fishing positions. It also allows the OLE to use 21st century technologies to monitor compliance, track violators, and provide substantial evidence for prosecution while maintaining the integrity of the individual fisherman's effort.

The system currently focuses its data mining capabilities on allowing U. S. Coast Guard personnel in OLE to utilize data to monitor and perform analysis intended to identify suspicious anomalies that could provide violations of laws that USCG regulate. The UCOP system is not designed to perform automated computations and has no user or other interfaces allowing inserts, updates, or deletion of data to be recorded to the UCOP databases.
More information addressing the Law Enforcement Sensitive aspects of this program are being provided in an annex to the report.

### 2. Technology and Methodology

USCG UCOP and the Vessel Monitoring System (VMS), owned by NOAA, requires interconnection between the two systems for the express purpose of exchanging data. This is authorized in accordance to the Interconnection Security Agreement (ISA) and MOU between USCG and NOAA.
USCG OLE utilize data to monitor and perform analysis intended to identify suspicious anomalies.

### 3. Data Sources

The primary function of UCOP is to collect and consolidate various track data sources into a unified picture, commonly referred to as the COP. This consolidation allows users to make informed decisions using the Tactical Decision Aids (TDA's) provided to them by the UCOP about operations in their area of operations and the units and commercial/private vessels within it.

The UCOP provides additional track attribute data about a vessel that may or may not have been available to the system user and allows the user to update/edit that attribute information (and making that information available to others seamlessly) such as NOAA data for shipping vessels (vessel type, such as a trawler, whaler, etc., and the country of origin), and Automated Identification System (AIS) data on shipping and land-based vessels, including their Maritime Mobile Service Identity (MMSI) number, country of origin, cargo, length, width and draft of vessel, next port of call, and whether the vessel is underway or anchored.

### 4. Efficacy

In FY 2019, USCG boarding teams discovered violations on approximately 80% of vessels targeted after comparing active VMS, historical VMS, vessel permits, and Marine Information for Safety and Law Enforcement (MISLE) history. Many of these violations were of a nature that would not be detected at a pier, such as fishing for a species that required a specific VMS code without the vessel declaring the code.[142]

### 5. Laws and Regulations

The Magnuson-Stevens Conservation and Management Act[143] authorizes the collection of reliable data essential to the effective conservation, management, and scientific understanding of the fishery resources of the United States.[144] Data is collected for implementation of a standardized fishing vessel registration and information management system[145] which houses identification data for fishing vessels and basic fishery performance data.[146] Data processed between the USCG UCOP and NOAA VMS systems are categorized as SBU.

---

[142] Vessels would fish until they were full, and then decide which VMS code to request from NOAA that best fit their catch for the day. Legally, the vessel is to request a code from NOAA prior to leaving the pier and fish accordingly to the code, not the other way around.
[143] 16 U.S.C. §§ 1801 et seq.
[144] 16 U.S.C. §§ 1801(a)(8).
[145] 16 U.S.C. §§ 1881.
[146] *Id*.

### 6. Privacy Impact and Privacy Protections

UCOP collects data from various sources within the USCG, but only utilizes limited data elements from each system to enable them to identify vessels or aircraft. UCOP collects the MMSI number but does not link PII such as vessel owner name, e-mail or home address, or emergency contact. The MMSI number, while linkable to an individual if combined with other PII, is not considered PII in the UCOP because users cannot access any additional data to link back to an individual.

As a necessary element, UCOP receives data from NOAA necessitating a MOU, ISA, and Memorandum Clarification of Responsibility for Securing Non-Disclosure Agreements (NDA) Before NOAA VMS Tracks.[147] In 2014, UCOP underwent a PTA to assess whether there is a need for additional Privacy compliance documentation; it was determined that no additional documentation was required. Additionally, UCOP has developed a System Privacy Plan (SPP) based upon a review of the system, documentation, DHS regulations/guidance, and interviews with the information system and privacy personnel.

The UCOP is the only authorized path for VMS data from NOAA to USCG. The NOAA feed to UCOP is a truncated version of the NOAA Office of Law Enforcement VMS data, which is limited to position, location, and identification (PLI). The MOU between the USCG and NOAA, dated May 10, 2017, establishes the requirements for data exchange between the two organizations. The MOU addresses communications, security incidents, disasters and other contingencies.

The ISA between the USCG and NOAA, dated October 6, 2016, establishes the technical requirements of interconnected IT systems. The requirements for interconnection between the two systems is for the express purpose of exchanging data between the UCOP owned and operated by USCG, and the VMS owned by NOAA. The USCG requires the use of NOAA VMS as a transport system for querying for VMS data in the NOAA database. As a matter of Coast Guard policy, and in consultation with NOAA Fisheries, VMS data is being shared by NOAA Fisheries with the USCG for the specific purposes of Fisheries Law Enforcement and Search and Rescue.
Both organizations ensure that adequate system access controls are in place and maintained on all components connected to the systems. The buildings that house the NOAA and UCOP servers are occupied by NOAA employees or Coast Guard personnel and are not open to the general public. These structures are either part of NOAA federal buildings or located on Coast Guard bases.

Both parties ensure that all individuals using the systems have attended initial basic and annual refresher *Computer Security Awareness and Training* and *Privacy Awareness Training*. Additionally, both parties ensure that persons with significant security responsibilities for the systems receive annual role-based training covering their specific areas of responsibility.

[147] COMDT (CG-7612), 5510 dated June 26, 2018.

## Conclusions

The DHS Privacy Office is pleased to provide Congress its fourteenth comprehensive report on DHS data mining activities. Congress authorized the Department to engage in data mining in furtherance of the DHS mission while protecting privacy.

The DHS Privacy Office reviewed the programs and systems described in this report utilizing its compliance documentation process to ensure necessary privacy protections are implemented. The DHS Privacy Office remains vigilant in its oversight of all Department programs and systems, including those that involve data mining.

## 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 Import Cargo | 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 |
| COP | Common Operating Picture |
| COTP | Captains of the Port |
| COTS | Commercial Off the Shelf |
| 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 |
| DoD | U.S. Department of Defense |
| 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 |

| Acronym List | |
|---|---|
| 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 |
| 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 |
| GCCS-J | Global Command and Control System - Joint |
| 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 |
| ISA | Interconnection Security Agreement |
| ISAA | Information Sharing and Access Agreement |
| IT | Information Technology |
| LES | Law Enforcement Sensitive |
| MDA | Maritime Domain Awareness |
| MISLE | Marine Information for Safety and Law Enforcement |
| MOA | Memorandum of Agreement |
| MSB | Money Services Business |
| NARA | National Archives and Records Administration |
| NCIC | National Crime Information Center |
| NIIS | Non-immigrant Information System |
| NOAA | National Oceanic and Atmospheric Administration |
| NTC | National Targeting Center |
| NTC-C | National Targeting Center-Cargo |
| OBIM | Office of Biometric Identity Management |
| OLE | Office of Law Enforcement |
| OMB | Office of Management and Budget |
| PCR | Privacy Compliance Review |

| Acronym List | |
|---|---|
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PLI | Position, Location, Identification |
| 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 |
| 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 |
| UCOP | Unclassified Common Operating Picture |
| 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 |
| VMS | Vessel Monitoring System |
| VSPTS-Net | Visa Security Program Tracking System |
| VWP | Visa Waiver Program |