Department of Homeland Security

2020 and 2021 Data Mining Report

August 2022

Homeland Security

Message from the Chief Privacy Officer

August 24, 2023

I am pleased to present the U.S. Department of Homeland Security's (DHS) "2021 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 activity's impact on privacy and protections in place to guard privacy. This is the fifteenth comprehensive DHS Data Mining Report and the thirteenth 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 a rigorous compliance process that 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 safeguard privacy.

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

Sincerely,

Mason C. Clutter
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 Kamala Harris
President of the Senate

The Honorable Kevin McCarthy
Speaker of the House of Representatives

The Honorable Gary C. Peters
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rand Paul
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Richard J. Durbin
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Lindsey O. Graham
Ranking Member, U.S. Senate Committee on the Judiciary

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

The Honorable Marco Rubio
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Patty Murray
Chairwoman, U.S. Senate Committee on Appropriations

The Honorable Susan Collins
Vice Chairwoman, U.S. Senate Committee on Appropriations

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

The Honorable Tim Scott
Ranking Member, U.S. Senate Committee on Banking, Housing and Urban Affairs

The Honorable Mark E. Green
Chairman, U.S. House of Representatives Committee on Homeland Security

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

The Honorable James Comer
Chairman, U.S. House of Representatives Committee on Oversight and Accountability

The Honorable Jamie Raskin
Ranking Member, U.S. House of Representatives Committee on Oversight and AccountabilityAccountability

The Honorable Jim Jordan
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Jerrold Nadler
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Michael Turner
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

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

The Honorable Kay Granger
Chairwoman, U.S. House of Representatives Committee on Appropriations

The Honorable Rosa DeLauro
Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Patrick McHenry
Chairman, U.S. House of Representatives Committee on Financial Services

The Honorable Maxine Waters
Ranking Member, U.S. House of Representatives Committee on Financial Services

Table of Contents

I. EXECUTIVE SUMMARY

The DHS Privacy Office provides 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 information required by the Act's reporting requirements for data mining activities.

This year's report provides updates on additions, modifications, and other developments to the following Departmental programs that engage in data mining, as defined by the Act, included in the last published DHS Data Mining Report:[2]

- 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 (AES) cargo, passengers (Unified Passenger [UPAX]), land border crossings (ATS-L);
- 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);
- ATLAS, which is administered by the U.S. Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security Directorate (FDNS);
- The Global Command and Control System – Joint (GCCS-J), which is administered by the U.S. Coast Guard (USCG); and
- Unclassified Common Operating Picture (UCOP), which is administered by the USCG.

Previous reports provided descriptions of the ICE FALCON-Roadrunner system and CBP SOCRATES Pilot Program, which were decommissioned in 2019, and the DHS Data Framework. As described in the 2018 Data Mining Report,[3] the Data Framework (currently called the "Data Services Branch") is not using a data mining capability. During implementation, the purpose of the project changed from the initial vision of a central authoritative, managed, curated, and governed data system to a managed data platform allowing purpose-built data services in support of DHS component analytical uses. If the Data Services Branch engages in data mining as defined by the Act, the DHS Privacy Office will provide details on the Data Services Branch data mining activities in future Data Mining Reports.

The 2019 DHS Data Mining Report was published in December 2020. The DHS 2020 Data Mining

[1] 42 U.S.C. § 2000ee-3.
[2] 2019 DHS Data Mining Report, issued in December of 2020, *available at*: https://www.dhs.gov/sites/default/files/publications/2019_data_mining_report_final_12-2-20.pdf
[3] 2018 DHS Data Mining Report, issued in November of 2019, *available at*: https://www.dhs.gov/sites/default/files/publications/2018-dataminingreport.pdf

Report to Congress was not submitted as planned. Accordingly, this 2021 Report also covers information that would have been reported in the 2020 Report. To ensure completeness, the Privacy Office conducted a gap analysis of the 2019 and 2021 Report data call results, including an assessment of whether any data mining efforts were initiated during the reporting periods. The Privacy Office determined that no data mining activity operated solely within 2020. DHS is currently compiling the 2022 Report.

This report, covering the period of January 1 through December 31, 2021, in addition to 2020, provides updates on additions, modifications, and other developments to the above referenced programs. The DHS Privacy Office identified an additional Departmental program that engages in data mining, as defined by the Act: Continuous Immigration Vetting for Operation Allies Welcome, utilizing ATS, conducted by CBP.

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

The *Homeland Security Act of 2002* expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[4] DHS exercises this authority with respect to programs discussed in this report, all of which have been reviewed for their potential impact on privacy by the DHS Chief Privacy Officer.

The Chief Privacy Officer's authority to evaluate 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."[5]

The DHS Privacy Office implements the Chief Privacy Officer's authorities through privacy compliance policies and procedures based, in part, on a set of eight Fair Information Practice Principles (FIPPs), rooted in the tenets of the Privacy Act of 1974.[6] The FIPPs serve as DHS's core privacy framework, as set forth in the Privacy Policy and Compliance Directive 047-01 and memorialized in the *Privacy Policy Guidance Memorandum 2008-0,1*[7] *The Fair Information Practice Principles: Framework for Privacy Policy at the U.S. Department of Homeland Security (December 29, 2008).*[8]

As described below, the DHS Privacy Office's privacy compliance process requires DHS components and offices that use systems and manage programs that collect, ingest, maintain, and

[4] 6 U.S.C. § 121(d)(11).
[5] 6 U.S.C. § 142(a)(1).
[6] 5 U.S.C. § 552a.
[7] Directive 047-01 and its accompanying Instruction are *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] 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.

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 System of Records Notice (SORN). The Privacy Office uses the PTA to determine whether a department program or system affects privacy, and if so, whether additional privacy compliance documentation is required.

Programs or systems that affect privacy (e.g., electronic systems where information in identifiable form is collected by DHS) may require publication of a PIA, as mandated by the *E-Government Act of 2002*[9] or required pursuant to the Chief Privacy Officer's statutory authority at 6 U.S.C. § 142, and/or a SORN in the Federal Register, as mandated by the *Privacy Act of 1974*,[10] before they become operational. All programs discussed in this report issued new or updated PIAs or are in the process of doing so; all are covered by DHS SORNs.

While each program described below engages in data mining to some extent, the DHS Privacy Office confirmed no decisions regarding individuals are made based solely on data mining results. In all cases, DHS employees analyze data mining results and apply their own judgment and expertise, including assessing corroborating information, in making determinations about individuals who may have been initially identified through data mining activities. The DHS Privacy Office works closely with each program to ensure required privacy compliance documents are current, personnel receive appropriate privacy training, and privacy protections are implemented and followed.

[9] 44 U.S.C. § 3501, note Section 208 of the E-Government Act.
[10] 5 U.S.C. § 552a(e)(4).

II. LEGISLATIVE LANGUAGE

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 Appropriationsand 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—

i) the detection of fraud, waste, or abuse in a Government agency or program; or

ii) 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 on 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 emphasized here. 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 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 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 2008-01/Privacy Policy Directive 140-06,[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 PII at the Department in fulfilment of the Department's mission to preserve, protect, and secure the homeland. The DHS Privacy Office also applies the FIPPs to DHS activities that involve data mining.

DHS's production of the Data Mining Report requires in-depth coordination with several offices and components. To ensure completeness in reporting, the DHS Privacy Office surveys components for any activities that could include data mining and audits DHS's internal tracking system. In some instances, reported activities are maintained in law enforcement sensitive or classified systems, which require greater care and collaboration to ensure proper reporting.

DHS uses three mechanisms to assess and ensure privacy compliance for DHS activities that involve data mining: (1) the PTA;[14] (2) the PIA;[15] and (3) the SORN.[16] Each document has a distinct function in the DHS privacy compliance framework. Together, they promote transparency and accountability.

To fulfill the Act's requirements, the DHS Privacy Office identifies DHS programs that engage in data mining through the Office's routine compliance oversight activities and use of targeted activity questionnaires focusing on data mining attributes. Additionally, the DHS Privacy Office reviews the Department's major IT budget submissions to the Office of Management and Budget (OMB) to

[12] Privacy Policy Directive 140-06, *available at*: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.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 document required by DHS policy that serves as the official determination by the DHS Privacy Office about whether a Departmental program or system affects privacy, 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, consistent with the protection of classified and other sensitive information.
[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).

gain knowledge of programs or systems that use PII and to determine whether they appropriately address privacy.[17] The DHS Privacy Office also evaluates PTA submissions to review all information technology systems 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 and mitigation strategies.

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 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.

[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 Execution of the Budget, *available at*: https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf. The term "major" is defined by the OMB Circular and DHS Directive 102-01 Rev 03.1. DHS designates programs as Major Level 1 and Level 2 based on the following dollar thresholds: Level 1 Major: (LCCE >$1 billion) and Level 2 Major: (LCCE $300 million - <$1 billion).

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

IV. Reporting

In the 2019 DHS Data Mining Report,[19] the DHS Privacy Office discussed the following Departmental programs and systems 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 (AES) cargo, land border crossings (ATS-L), and passengers (UPAX);
- 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);
- ATLAS, which is administered by the U.S. Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security Directorate (FDNS);
- 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.

This section of the 2020 and 2021 report presents complete descriptions of these programs together with updates on any modifications, additions, and other developments that occurred in the current reporting year. In addition, the DHS Privacy Office identified an additional Departmental program that engages in data mining, as defined by the Act: Continuous Immigration Vetting for OAW, utilizing ATS, conducted by CBP.

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

[19] 2019 DHS Data Mining Report, *available at* https://www.dhs.gov/sites/default/files/publications/2019_data_mining_report_final_12-2-20.pdf.

A. Automated Targeting System (ATS)

2021 Program Update

CBP operates the UPAX decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data. Within UPAX, an automated targeting system 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 2021 reporting period, CBP made no modifications or updates to the vetting of other populations on which DHS previously reported. As will be discussed in later reports, CBP published an ATS PIA Addendum Update during the 2022 reporting period to notify the public of additional populations for which ATS will be used. The expanded populations include Continuous Immigration Vetting for Operation Allies Welcome.

1. Continuous Immigration Vetting for Operation Allies Welcome

UPAX is used to continually vet potential Special Immigrant Visa eligible Afghans, including those who worked alongside United States personnel in Afghanistan, as they seek to resettle in the United States under Operation Allies Welcome. Prior to any Afghan national's arrival at a U.S. port of entry as part of Operation Allies Welcome, the U.S. government conducted biometric and biographic screening and vetting of these individuals to protect national security, border security, homeland security, and public safety. After receiving this initial vetting overseas, Afghans who arrive at a U.S. port of entry present themselves to a CBP officer for inspection.

Pursuant to 8 U.S.C §1182(d)(5), the Secretary of DHS has authority and discretion to temporarily parole into the United States, only on a case-by-case basis, under such conditions as the Secretary may prescribe for urgent humanitarian reasons or significant public benefit, any noncitizen applying for admission to the United States who would otherwise be inadmissible. Under Operation Allies Welcome, CBP may, on a case-by-case basis, temporarily parole into the United States eligible Afghans for up to two years and issue Form I-94, Arrival/Departure Record.[20] However, pursuant to the Immigration and Nationality Act (INA) § 212(d)(5)(A), an individual who is paroled into the United States is not legally admitted into the United States despite being permitted to physically enter the country. Parole may be terminated, pursuant to 8 C.F.R. § 212.5(e), among other reasons, when an authorized official determines that neither humanitarian reasons nor public benefit warrants the continued presence of the parolee in the United States.[21]

---

[20] *See* U.S. Department of Homeland Security, U.S. Customs and Border Protection, Privacy Impact Assessment for the I-94 Website Application, DHS/CBP/PIA-016, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[21] While this report covers 2020 and 2021 data mining activities, it is published in 2023. Accordingly, DHS notes that the ATS PIA Operation Allies Welcome Addendum was updated on June 12, 2022, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection; DHS/CBP/PIA-006 Automated Targeting System | Homeland Security

CBP uses UPAX to run Continuous Immigration Vetting (CIV) on individuals paroled into the United States under Operation Allies Welcome. UPAX contains a consolidated list of the biographic data elements collected during the initial vetting processes, information from USCIS Form I-765,[22] and CBP historical holdings to timely identify derogatory information for the two-year timeframe the individual is paroled into the United States. This information is continuously vetted for law enforcement, border security, national security, and counterterrorism purposes for the two-year parole period granted to most individuals under Operation Allies Welcome. Matches to derogatory information are considered on a case-by-case basis to determine if parole should be terminated pursuant to 8 CFR § 212.5(e).

CBP's ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107- 173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). See also, e.g., 6 U.S.C. §§ 111, 211; 8 U.S.C. §§ 1103, 1182, 1225, 1225a, 1324; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, 1644a.

2. Non-Immigrant and Immigrant Visa Applications

As described in the 2012 ATS PIA,[23] subsequent PIA updates, and reported in previous DHS Data Mining Reports,[24] UPAX is used to vet non-immigrant visa applications for the U.S. Department of State (DoS). In January 2013, CBP and DoS began pre-adjudication investigative screening and vetting for 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 visa applications and provides a response to the DoS's Consular Consolidated Database (CCD)[25] indicating if DHS 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 is determined without further research, or additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net)[26] 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*

[22] Certain noncitizens who are in the United States may file Form I-765, Application for Employment Authorization, to request employment authorization and an Employment Authorization Document (EAD). Other noncitizens whose immigration status authorizes them to work in the United States without restrictions may also use Form I-765 to apply to USCIS for an Employment Authorization Document that shows such authorization.
[23] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates, *available at* https://www.dhs.gov/privacy.
[24] 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.
[25] *See* the CCD PIA, *available at:* https://www.yumpu.com/en/document/view/18950697/consular-consolidated-database-ccd-pia-us-department-of-state.
[26] *See* DHS/ICE/PIA-011 Visa Security Program Tracking System (VSPTS-Net), *available at:* https://www.dhs.gov/privacy.

Reform Act of 2002 (EBSVERA) authorizes the use of UPAX for screening non-immigrant and immigrant visas.[27]

3. Enhanced Overstay Validation and Biographic Exit

Since 2013, the Arrival and Departure Information System (ADIS)[28] has enabled DHS to better track overstays by compiling information from a variety of federal systems to create a complete travel profile of an individual using their travel history.[29] To calculate a complete travel history for an individual and determine whether an individual violated terms of admission into the United States, ADIS collects arrival and departure information, class of admission information, and immigrant benefit information from external sources to determine whether an individual is an overstay.

ADIS aggregates the following data from various systems to create a person-centric view of a traveler to determine full travel history:

- Date the individual entered the United States;
- Class of admission;
- Updates or changes to the individual's immigration status; and
- When available, the date the individual departed the United States.

ATS, as a part of the Enhanced Overstay Validation and Biographic Exit effort, is used to vet potential visa and non-visa overstay candidates based on supporting data available in multiple CBP systems. ADIS generates overstay leads based on information from source systems, which are then sent to ATS and enriched with border crossing information (derived from DHS/CBP's Border Crossing Information (BCI) system),[30] Form I-94 Notice of Arrival/Departure records (derived from DHS/CBP's Nonimmigrant Information System (NIIS)),[31] and data from the DHS/ICE Student Exchange Visitor Information System (SEVIS).[32] ATS prioritizes the list using targeting rules and sends a remaining viable overstay list to ICE to locate high-risk overstays and initiate criminal investigations or removal proceedings against those individuals.

---

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

[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] An overstay is a nonimmigrant who was lawfully admitted to the United States for an authorized period but remained in the United States beyond their authorized period of admission. The authorized admission period can be a fixed period, or for the duration of a certain activity, such as the period during which a student is pursuing a full course of study or any authorized technical/practical training.

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

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

[32] *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.

The principal legal authorities that support DHS's maintenance, use, and sharing of ADIS information as an entry and exit program necessary to identify foreign nationals who remain in the United States beyond their authorized period of admission include: Title 6 of the United States Code, Domestic Security; Title 8 of the United States Code, Aliens and Nationality; Title 42 of the United States Code, The Public Health and Welfare (Reporting information to the Social Security Administration); Homeland Security Presidential Directive 6, Integration and Use of Screening Information (September 16, 2003); Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003); Homeland Security Presidential Directive 11, Comprehensive Terrorist-Related Screening Procedures (August 27, 2004); and Executive Order No. 13880, on Collecting Information about Citizenship Status in Connection with the Decennial Census (July 11, 2019), 84 FR 33821 (July 16, 2019).

4. Trusted Traveler and Trusted Worker Vetting

The vetting process for CBP's Trusted Traveler Programs and Trusted Worker populations 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 utilized to determine applicant eligibility for 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 renewed Trusted Traveler applications was fully transitioned to the ATS platform as part of the TECS system Modernization effort to interface with the modernized Department of Justice's (DOJ) National Crime Information Center (NCIC) and National Law Enforcement Telecommunications System (NLETS) queries.[33] ATS provides improved vetting algorithms designed to assist in identifying more refined matches to derogatory records. Results of the vetting analysis provide a consolidated view of applicant 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 on this capability in March 2016. In FY 2017, CBP enabled a recurrent vetting process beyond initial submission for individuals with trusted traveler membership through the ATS platform. Additionally, since FY 2017, CBP has enabled Ports of Entry to use the ATS platform to vet Trusted Worker applicants.

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

[33] TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC) Terrorist Screening Dataset TSDSSet (TSDS), 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).

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; 6 U.S.C. § 211; 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.

5. Special ATS Programs

a) ATS Enhancements to Command and Control Services (C2S) (formerly known as Watchkeeper)[34]

C2S is a USCG application in which port security information is coordinated and organized to improve tactical decision-making, situational awareness, operations monitoring, rules-based processing, and joint planning in a coordinated interagency environment. C2S provides a fully functioning and shared common operational picture, shared mission tasking, and shared response information sets to all users within the Interagency Operations Center (IOC) with USCG Network access. The C2S environment provides the service infrastructure to share data with external systems outside of the C2S. C2S's data is presented to Coast Guard users with access to Coast Guard One View, including partner federal agencies and local port partners.

USCG C2S integration of the ATS Import Cargo and UPAX modules, discussed below, serve as tools to conduct pre-arrival screening and vetting of vessel cargo, crew, and passengers. ATS-enhanced C2S provides near real-time data for Captains of the Port (COTP) to better evaluate threats and deploy resources through active collection of incoming vessel information. With a more detailed picture of the risk profile 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 C2S include the Security and Accountability for Every Port (SAFE Port) Act of 2006, 46 U.S.C. § 70107A; 5 U.S.C. § 301; 14 U.S.C. § 632; 33 U.S.C. §§ 1223, 1226; 46 U.S.C. §§ 3717, 12501; Section 102 of the Maritime Transportation Security Act of 2002, Pub. L. No. 108-274; Section 102(c) of the Homeland Security Act, 14 U.S.C. § 2; 33 C.F.R. part 160; and 36 C.F.R. chapter XII.

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 collection, use, analysis, and dissemination of information gathered for targeting, identifying, and preventing potential terrorists and terrorist

[34] The DHS Privacy Office and USCG published a PIA for Watchkeeper on January 4, 2013; however, the Watchkeeper PIA will be updated to discuss the renamed C2S system and its functionality. 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.

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 travelers, conveyances, and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data, so these data elements are 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 (air passengers and crew on international flights, and passengers and crew on international sea carriers), private vehicles and travelers crossing at land borders, and provides a workspace to support creation and retention of analytical reports. This report discusses the following modules: ATS Import Cargo and AES (both of which involve the analysis of cargo), ATS (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 import or export 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 AES became operational in 1997. UPAX became operational in 1999 and is now even more critical to CBP's mission.

ATS Unified Passenger allows CBP officers to determine whether a variety of potential risk indicators exist for travelers that may warrant additional scrutiny. Unified Passenger 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).[37]

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

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

Visa Update System (EVUS),[38] Global Enrollment System (GES), the Nonimmigrant Information System (NIIS), BCI, Seized Assets and Case Tracking System (SEACATS), ICE's SEVIS and Enforcement Integrated Database (EID), and TECS.[39] TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[40] Terrorist Screening Data Set (TSDS) 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. ports), entries, and entry summaries for cargo imports; Electronic Export Information (EEI) (formerly referred to as Shippers' Export Declarations) submitted to the AES and transportation bookings and bills for cargo exports; manifests for arriving and departing travelers; 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 TSDS 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 offers a graphical user interface for many 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 is restricted by existing technical security and privacy safeguards associated with the source systems.

---

[38] 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 C.F.R. § 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 or she deems necessary for carrying out his or her authority. CBP has no modifications or updates to EVUS since 2016.

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

[40] 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 TSDS.

Many rules are included in the ATS modules, which allow CBP officers to analyze sophisticated concepts of business activity and 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 Outbound Cargo Targeting Models

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 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 to target cargo for possible violations of U.S. law. 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. 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. 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 use of advanced algorithms in support of its mission.[41] To that end, as discussed in previous DHS Data

[41] 6 U.S.C. § 943(e)(2).

Mining Reports, CBP established an Advanced Targeting Initiative (ATI), which employs development of data mining, machine learning,[42] 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 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 information is either submitted by private entities or persons and initially collected in DHS/CBP source systems (e.g., ACE). 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,

[42] 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.

automated assessment of the risk of each import.[43] AES 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 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. Results of ATS Import Cargo and AES analyses identifying cargo as suspicious were regularly corroborated by physical searches.

In 2021, NTC-CD used ATS to target and refer 327 shipments to various ports of entry that led to narcotic seizures, including 49 seizures of Fentanyl, and 16,800 kilograms of precursor chemicals. NTC-CD used AES to target and refer 178 export shipments to various ports that led to seizures, including satellite antennas destined to Russia, stolen vehicles to Africa, and stolen sensitive technology destined to China.

In November 2021, NTC-CD identified through ATS an express consignment shipment manifested as "Making Machine" to CBP officers in Cincinnati and referred it for inspection. Additionally in November 2021, CBP officers in Cincinnati notified the CBP NTC that the shipment was positive for a pill press, motor, and parts. The consignee was part of a Drug Enforcement Agency investigation that resulted in significant arrests, seized chemicals, seized currency, seized drugs, seized property, seized vehicles, and seized weapons.

5. Laws and Regulations

There are numerous customs and related authorities authorizing collection of data regarding import and export of cargo and entry and exit of conveyances.[44] AES and ATS Import Cargo also support functions mandated by Title VII, Counterterrorism and Drug Law Enforcement, of Public Law 104-208 (Omnibus Consolidated Appropriations Act, 1997), which provides funding for counterterrorism and drug law enforcement. AES also supports functions arising from the Anti-Terrorism Act of 1987[45] and the 1996 Clinger-Cohen Act.[46] Risk assessments for cargo are also mandated under Section 912 of the SAFE Port Act.[47]

[43] ATS-N collects information from source systems regarding individuals in connection with, for example, bills of lading.
[44] *See, e.g.*, 19 U.S.C. §§ 482, 1415, 1431, 1433, 1461, 1496, 1499, 1581-1583; 22 U.S.C § 401; and 46 U.S.C. § 46501.
[45] 22 U.S.C. §§ 5201 *et seq.*
[46] 40 U.S.C. §§ 1401 *et seq.*
[47] 6 U.S.C. § 912(b).

ii. ATS-Unified Passenger

1. Program Description

ATS Unified Passenger is a custom-designed system used at the NTC, U.S. ports of entry, and by authorized users stationed abroad particularly those receiving international flights (both commercial and private) and voyages, and at the CBP NTC-CD to evaluate passengers and crew members prior to arrival and departure. UPAX facilitates CBP officer decision-making processes 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. UPAX is a fully operational application that utilizes CBP's System Engineering Life Cycle methodology[48] and is subject to recurring systems maintenance.

2. Technology and Methodology

UPAX processes traveler information, as well as visa, ESTA, EVUS, and GES information against other information available through ATS. ATS UPAX 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. Updates to ATS that comprise UPAX involve a cleaner visual presentation of relevant information used in vetting and inspection processes. 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 to support information query capability and allow relevant data to be consolidated or accessed from the primary screen used to vet targeting results pertaining to a traveler or applicant.

ATS UPAX continues to rely on risk-based rules derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. Unlike in the cargo environment, UPAX does not use a score to determine an individual's risk level; instead, UPAX compares information available through ATS against watch lists, criminal records, warrants, and patterns of suspicious activity identified through past investigations. Results of these comparisons are either assessments of 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

[48] CBP's Office of Information & Technology's System Engineering Life Cycle (SELC) is a policy that establishes 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.

or further focus those rules to improve the effectiveness of their application.

Results of queries in UPAX are designed to signal to CBP officers that further inspection of a person may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise noted as a person of concern to law enforcement. Risk assessment analysis is generally performed in advance of a traveler's arrival in or departure from the United States and is 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, UPAX is used by CBP officers for decision support. Officers do not make decisions about individuals solely based on the automated results of data mining of information available through UPAX. Rather, the CBP officer uses the information in UPAX to assist in determining whether an individual should undergo additional inspection based on the totality of the circumstances.

3. Data Sources

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

4. Efficacy

Unified Passenger provides information to its users in near real-time. The flexibility of Unified Passenger'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 Unified Passenger greatly increases efficiency and effectiveness of officers' eliminating the need for 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 information generated by Unified Passenger to aid decision-making about risks associated with individuals. As discussed below, ATS includes real-time updates of information from source systems to ensure CBP officers act on accurate information.

In this reporting period, Unified Passenger identified, through lookouts and/or risk-based rule sets, individuals who were confirmed matches to the TSDS resulting in further inspection or, in some cases, recommendations to carriers not to board such persons. Unified Passenger matches have also enabled CBP officers and foreign law enforcement partners to share information and disrupt or apprehend persons engaged in trafficking and smuggling operations.

For example, during vetting of certain Afghan nationals under Operation Allies Welcome, CBP Officers identified an individual as a national security risk. Through facial comparison technology and enrichment information in ATS, CBP identified the subject along with his immediate family members as positive matches to records related to national security concerns.

In addition, CBP officers using ATS identified an individual departing the United States without proper travel authorization, who was considered a potential high risk for technology transfer. Based

on research, the subject was referred for an outbound inspection as he attempted to depart and was subsequently found to possess unauthorized sensitive technology and research. CBP officers detained and seized all electronics in the individual's possession.

Additionally in 2021, CBP officers using ATS identified an individual seeking admission into the United States at a designated foreign pre-clearance location, who was considered high-risk due to national security related concerns. Based on available information, the traveler was referred for inspection. The individual was found inadmissible due to information discovered during inspection combined with information previously known. The traveler was refused admission under the Visa Waiver Program and did not board the flight to the United States.

In addition, CBP officers using ATS identified a traveler with a J1 visa seeking admission into the United States at a U.S. port of entry who was considered a potential high risk for violation of the Immigration and Nationality Act, including possible visa fraud and/or traveling to the United States for purposes of facilitating illicit technology transfers. Based on available information and information discovered by CBP during inspection, the traveler was expeditiously removed from the United States.

5. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing the United States.[49] As part of this inspection and examination process, each traveler seeking to enter the United States must first establish their 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,[50] ATSA, IRTPA, the Immigration and Nationality Act (INA), and the Tariff Act of 1930, as amended.[51] Information collected in advance of arrival or departure is often found on routine travel documents that passengers and crew members present to a CBP officer upon arrival in or departure from the United States.

iii. 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,[52] 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

[49] *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.
[50] 8 U.S.C. § 1721.
[51] 19 U.S.C. §§ 66, 1433, 1454, 1485, and 1624.
[52] *See* DHS/TSA/PIA-018(i) Secure Flight - Silent Partner and Quiet Skies. *available at* https://www.dhs.gov/privacy.

maintained by the Federal Government, enabling TSA to take appropriate actions to address and mitigate risk.

Under Silent Partner, TSA creates rules based on current intelligence for use by ATS to identify passengers for enhanced screening on international flights bound for the United States. Once identified by the rule, 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 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 TSDS under Homeland Security Presidential Directive 6 based solely on the fact their travel falls within a security rule. They may be nominated to the TSDS, however, if they are involved in a security incident that would meet TSDS nomination requirements.

2. Technology and Methodology

The Silent Partner and Quiet Skies programs utilize CBP's ATS to create lists of aviation passengers selected for enhanced screening based on risk-based intelligence-driven rules as part of TSA's Secure Flight program vetting process. 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 that used by a partially identified terrorist; or upon submitting passenger information matching that used by a known or suspected terrorist.

3. Data Sources

Information used by the system is initially provided by individual passengers to airlines (or to reservations agents). ATS collects and retains passenger information entering or departing the United States in accordance with legal requirements for individuals making 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 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 Identification; 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 an authorized ATS user, TSA can access information about an individual 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 maintains 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 existing threats to aviation security implementing additional measures to mitigate threats 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 reviews TSA conducted following the December 25, 2009, attempted airline attack, designate higher risk passengers using intelligence-based rules, ensuring enhanced screening of such passengers prior to boarding flights to and within the United States.

In 2014, Silent Partner identified a terrorist for enhanced screening who used biographic information not contained within the TSDS 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 some passengers were independently added to the TSDS as known or suspected terrorists after being designated for enhanced screening by Quiet Skies. Because TSA does not use Silent Partner or Quiet Skies to nominate individuals to the TSDS, these additions came by some process other than TSA action or analysis. While matching a Silent Partner or Quiet Skies rule does not indicate that an individual should be on the TSDS, this analysis indicates rules successfully identify passengers whose travel shows a higher-than-normal risk.

5. Laws and Regulations

TSA's general operating authorities are set forth in the *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 responsibility from air carriers for 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 DHS to compare passenger information for international flights to and from the United States against consolidated and integrated terrorist watch lists 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 watchlists, when warranted by security considerations, TSA may screen against the full TSDS 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. 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 review of and oversight for TSA's intelligence-driven, risk-based screening rules, and requires TSA and the DHS Traveler Redress Inquiry Program (DHS TRIP) to ensure 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 their travel lifecycle.

c) ATS Privacy Impact and Privacy Protections

The DHS Privacy Office works closely with CBP to ensure ATS satisfies privacy compliance requirements for operation. As noted above, CBP updated the SORN for ATS in May 2012,[53] and continually updates DHS/CBP/PIA-006(e) ATS.[54] 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 risk-based targeting rules used in ATS to ensure the rules are appropriate, relevant, and effective, and assess whether privacy and civil liberties protections are adequate and

[53] DHS/CBP-006 Automated Targeting System, (May 22, 2012) 77 Fed. Reg. 30297.
[54] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 2017) and previous updates *available at* https://www.dhs.gov/privacy.

consistently implemented.

Authorized CBP officers and agents and personnel from DHS I&A, ICE, TSA, USCG, USCIS, and USSS 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.[55] ATS supports, but does not replace, decision-making responsibilities of CBP officers, agents, and analysts. Decisions made or actions taken regarding individuals are not based solely on results of automated searches of data in the ATS system. Information obtained in such searches assist CBP officers and analysts in 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 that provide direct support to CBP. Each agency enters a Memorandum of Understanding with CBP that specifies conditions on access to ATS and requirements to perform approved missions in support of CBP. This includes laws, policies, and procedures applicable to protection of PII. Other federal agencies have restrictions on what data is made available to them in ATS.

When PII (such as certain data within a PNR) used by or maintained in ATS 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.[56]

CBP created the CBP INFO Center in its Office of Public Affairs to serve as a clearinghouse for all redress requests that come to CBP directly and concern inaccurate information collected or maintained by its electronic systems, including ATS. This process is available even though ATS does not form the sole basis for identifying enforcement targets. To facilitate redress, DHS created a comprehensive Department-wide program, called 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 experienced during their travel screening and inspection.[57]

Under the ATS PIA and SORN, and as a matter of DHS policy,[58] CBP permits subjects of PNR data or their representatives to make administrative requests for access and amendments of the PNR

[55] Personnel from TSA, ICE, USCIS, USCG, USSS, 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.
[56] 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 CBP INFO Center address and the Joint Intake Center telephone number.
[57] DHS TRIP (Traveler Redress Inquiry Program) can be accessed at: https://www.dhs.gov/dhs-trip.
[58] https://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/262-16.pdf.

data. Procedures for individuals to request access to PNR data within ATS are outlined in the ATS SORN and PIA. These procedures mirror those provided for access in the source systems for ingested data, so individuals may request access to their own data from either ATS (if ATS is the source system) or source systems that provide input to ATS in accordance with the procedures set out in each SORN. 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.[59] FOIA, Privacy Act, and JRA requests for access to information for which ATS is the source system are directed to CBP.[60]

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 only appropriate individuals have access to the system. CBP's Office of Professional Responsibility also conducts periodic reviews of ATS to ensure the system is accessed and used in accordance with documented DHS and CBP policies. Access to data used in ATS is restricted to persons with a clearance approved by CBP, approved access to separate local area networks, 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. 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 record retention requirements of those systems.

The retention period for data maintained in ATS will not exceed fifteen years, except as noted below.[61] The retention period for PNR data, which is contained only in Unified Passenger, is subject to the following further access restrictions and masking requirements: Unified Passenger users with PNR data access have access to PNR data in an active status for up to five years, with the PNR data depersonalized and masked after the first six months of this period. After the initial five-year retention period in active status, the PNR data is transferred to a dormant status for a period of up to ten years. PNR data in dormant status is subject to additional controls including the requirement to obtain access approval from an appropriate CBP supervisor. Furthermore, PNR data in the dormant status may only be unmasked in connection with a law enforcement operation and

[59] 5 U.S.C. § 552; 5 U.S.C. § 552a; 5a; 5 U.S.C. § 552a note.
[60] To submit a FOIA request electronically to CBP, it must be submitted by visiting https://www.securerelease.us/.or mailed to FOIA Officer, U.S. Customs and Border Protection, 90 K Street, NE, FOIA Division, Washington, DC 20229.
[61] NARA approved the record retention schedule for ATS on April 12, 2008.

only in response to an identifiable case, threat, or risk.[62]

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

B. Analytical Framework for Intelligence (AFI)

2021 Program Update

In July 2021, the AFI PIA was updated to permit access to AFI by additional DHS components including the DHS Cybersecurity and Infrastructure Security Agency (CISA) Integrated Operations Division/Intelligence.[63]

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 with 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 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.

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 provides AFI analysts with different tools to identify non-obvious relationships. AFI allows analysts to generate finished intelligence products to better inform finished intelligence product users about why an individual or cargo is 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.

[62] 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.
[63] The PIA for AFI is available at: http://www.dhs.gov/privacy-impact-assessments.

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

AFI allows analysts to search several databases 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 results to AFI analyst in a manner that allows for easy visualization and analysis.

AFI enables AFI analysts to upload, index, and store relevant information from other sources, such as the Internet or traditional news media, subject to procedures described below. AFI creates an index of relevant data in existing operational DHS source systems by ingesting data to enable faster return of search results. Indexing engines refresh data from originating systems periodically depending on the source data system. AFI adheres to records retention policies of the source data systems along with user access controls. Finished intelligence products and unfinished "projects" 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 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 showing 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. AFI tracks where AFI analysts search and routinely audits these records. AFI analysts use data from commercial data aggregators to complement or clarify data. AFI provides a suite of tools that assist analysts in detecting trends, patterns, and emerging threats, and in identifying non-obvious relationships, using information maintained in the index and made accessible through federated queries.

AFI also serves as a repository that allows select users the ability to upload informational and/or intelligence reports. These reports are viewable by all AFI users with appropriate access and need to know and may be shared externally pursuant to routine uses described in the CIRS SORN.

2. Technology and Methodology

AFI creates and retains an index of searchable data elements in existing operational DHS source systems by ingesting data through and from source systems. The index indicates which source system records match search term used. AFI maintains an index of key data elements that, in context, are personally identifiable. Indexing engines regularly refresh data from source systems. Any changes to source system records, or addition or deletion of source system records, is reflected in corresponding amendments to the AFI index during routine updates.

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

Specifically, analyses 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 analysts identify patterns or associations in the data. This analysis can produce a time sequence of events.

Results are used to generate finished intelligence products and projects and are published in AFI for users to search. In all situations, research developed, or reports generated 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 a data source is not available due to technical issues, the AFI analyst is unable to retrieve a responsive record in its entirety. Additionally, AFI analysts may upload information they determine relevant to a project, including information publicly available on the Internet.

AFI uses, disseminates, or maintains seven categories of data containing PII.[64]

- *DHS-Owned Data that AFI automatically receives 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; Import Cargo, Trade Entity, TECS records, Border Crossing Information (BCI), Vehicle Crossings, NLETS queries captured on Primary, Foreign Border Crossing Records, Secure Flight Passenger Data, TECS Incident Report Logs and Search, Arrest, Seizure Reports, Primary Name Query, Primary Vehicle Query, Secondary Referrals, TECS Intel Documents; and visa data);
    - Select legacy Intelligence Fusion System (IFS) datasets (including the following

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

information: EID detention data,[65] ICE intelligence information reports, ICE intelligence products, ICE name trace, ICE significant event notification, Detention and Removal Leads, and TECS Reports of Investigation);[66]
    - Enterprise Management Information System-Enterprise Data Warehouse (including: Arrival and Departure Form I-94;[67] CMIR data;[68] apprehension, inadmissibility, and seizure information from the ICE Criminal Arrest Records and Immigration Enforcement Records (CARIER);[69] National Security Entry-Exit Program information from CARIER; SEVIS information;[70] and seizure information from the Seized Asset and Case Tracking System);[71] and
    - The ATS-Targeting Framework (event case information).
- *DHS-Owned Data to which AFI provides federated access*: This 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 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 available through ATS, such as identity and biographical information, Financial Crimes Enforcement Network (FinCEN) data, wants and warrants, DMV data, and data from the TSDS.[72] AFI also contains some limited foreign government data obtained via open source websites (specifically foreign criminal information).
- *Commercial Data*: AFI collects identity and imagery data from several commercial data aggregators so DHS AFI analysts can cross-reference information with that 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 information uploaded by an authorized user either as original content or from an ad hoc data source such as the Internet or traditional news media. AFI analyst-provided information such as textual data (official reports users have seen as part of their duties or segments of a news article), video and audio clips, pictures, or any other information the user determines is relevant. User-submitted RFIs and projects are also stored within AFI, as well as the responses to those requests.
- *AFI Analyst-Created Information*: AFI maintains user-created projects as well as finished

[65] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at:* https://www.dhs.gov/privacy.
[66] *See* DHS/ICE/PIA-007 Law Enforcement Intelligence Fusion System (IFS), *available at* https://www.dhs.gov/privacy.
[67] *See* DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS) *available at* https://www.dhs.gov/privacy.
[68] The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.
[69] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), (Oct. 19, 2016) 81 Fed. Reg. 72080.
[70] *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.
[71] DHS/CBP-013 Seized Assets and Case Tracking System, (Dec. 19, 2008) 73 Fed. Reg. 77764.
[72] *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.

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 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 related to those roles. Continued operational use of AFI provides improved information sharing amongst participating DHS components. In this reporting period, 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 criminal organizations. CBP officers used AFI's batch search capabilities to search several hundred entities (individuals and locations) across multiple CBP data sources much faster than they could without AFI. This provided officers more time to review responsive records and take appropriate action. In 2021, AFI enabled:

- Identification of an individual associated with a terrorist organization via a common contact phone number;
- Visualization and analysis of smuggling routes and associated subjects as well as relationships to other smuggling operations; and
- Identification and seizure of narcotics based on information and associations that were difficult to find in other systems.
- Identification of a migrant smuggler associated with a stash house.

5. Laws and Regulations

Numerous authorities mandate 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 built extensive privacy protections into the structure and governance of AFI.[73] AFI itself does not collect information directly from individuals and CBP does not use this information 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 use of their information, as appropriate. AFI provides public notice about its use of information through its PIA and CIRS SORN.[74]

AFI is designed and developed in an iterative, incremental fashion. CBP ensures AFI is built and used in a manner consistent with the Department's authorities, and information in AFI is used consistent with the purpose for which it was originally collected. CBP also evaluates the need to develop enhancements to AFI, reviews and approves innovative 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,[75] and December 6, 2016.[76]

Although AFI indexes information from many different source data systems, each source system maintains control of collected data even though it is also maintained in AFI. Accordingly, only DHS AFI analysts authorized to access data in a source system have access to that same data through AFI.[77] 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, users are required to complete annual training in privacy awareness. All CBP employees are required to have privacy training 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.

As noted, AFI does not collect information directly from the public or any other primary source. Therefore, data accuracy is dependent upon system(s) performing the original collection. DHS AFI analysts use a variety of data sources available through source systems to verify and corroborate available information to the greatest extent possible. Accuracy of DHS-owned data, other federal agency data, and data provided by commercial aggregators depends on the original source. DHS AFI analysts are required to make changes to 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 agency data or commercial data aggregators correct information, queries of those systems reflect corrected

[73] *See* DHS/CBP/PIA-010 AFI *available a*t http://https://www.dhs.gov/privacy.
[74] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, (September 21, 2017) 82 FR 44198.*available a*t http://https://www.dhs.gov/privacy.
[75] The 2014 AFI PCR is available at: https://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.
[76] The 2016 AFI PCR is available at: https://www.dhs.gov/sites/default/files/publications/AFI%20PCR%20final%2012062016.pdf.
[77] 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 may have access to AFI.

information.

To further mitigate the risk of AFI retaining incorrect, inaccurate, or untimely information, AFI routinely updates its index to ensure the most current data is available to its users. Any changes to the source system record, or addition or deletion of a source system record, is reflected in corresponding amendments to the AFI index when updated.

AFI 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 information is used in accordance with CBP policies and procedures. 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 data (e.g., For Official Use Only, Law Enforcement Sensitive), and based on need-to-know.

AFI was developed to meet Intelligence Community standards to prevent unauthorized access to data, ensuring 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 information assurance policies against which AFI was designed, developed, and tested (including DHS Directive 4300 A/B). In April 2017, AFI was granted ongoing authority to operate (OATO) from the DHS Office of the Chief Information Security Officer. Government systems accessed or used by AFI undergo 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 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 AFI SORN, to the extent a record is exempted in a source system, exemptions will apply in AFI. When there are no access exemptions for a record in a source system, CBP may provide access to information maintained in AFI.[78]

To the extent CBP accesses and incorporates information from other DHS systems of records as sources of information for finished intelligence products, CBP will abide by safeguards, retention schedules, and dissemination requirements of those underlying source systems of record. Consistent with the *DHS N1-563-07-016* records schedule (May 30, 2008), CBP retains information consistent with retention requirements of the DHS Office of Intelligence and Analysis:

[78] 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.

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 include 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 National Archives and Records Administration (NARA) after twenty (20) years.

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)

2021 Program Update

During the reporting period, ICE updated FALCON-DARTTS PIA to include compliance documentation for Student Exchange Visitor Information. This collection is not new to the system. The PIA update lists applicable compliance documentation in the PIA appendix. FALCON-DARTTS resides in the ICE Homeland Security Investigations (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.

ICE published the FALCON-DARTTS PIA on January16, 2014, and updated and published the FALCON Search & Analysis (FALCON-SA) Appendix to reflect specific datasets and analytical results from FALCON-DARTTS are ingested into FALCON-SA. On December 1, 2014, ICE republished the Trade Transparency Analysis and Research (TTAR) SORN, which applied to FALCON-DARTTS. On March 22, 2021, the TTAR SORN was consolidated into the DHS/ICE-018 Analytical Records SORN.

Additional information about FALCON-DARTTS is included in an annex to this report that contains law enforcement sensitive 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 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 HSI is responsible for investigating, such as smuggling. Pursuant to their mission, HSI investigators and analysts must understand 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 analysis and identification of anomalies for investigators.

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. 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 anomalous transactions to determine if they are suspicious and warrant further investigation. HSI special agents gather additional facts, verify accuracy of FALCON-DARTTS data, and use their judgment and experience to decide whether to investigate further. Not all anomalies lead to formal investigations.

FALCON-DARTTS is used by HSI special agents and intelligence research specialists who work on TTU investigations at ICE Headquarters and in the ICE HSI field and foreign attaché offices, as well as properly cleared support personnel. In addition, select CBP personnel and foreign government partners have limited access to FALCON-DARTTS. CBP customs officers and import specialists who conduct trade transparency analyses in furtherance of CBP's mission use 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 established TTUs and 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, 31 U.S.C. §§ 5311-5332; 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 and provided by the U.S. Department of the Treasury's 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 associated with a user's specific profile that has legal authority to access. Specifically, only ICE HSI and CBP users are granted access to law enforcement data, and only ICE HSI users are granted access to financial data maintained in FALCON's general data storage environment. In this environment, 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 Reports of International Transportation of Currency or Monetary Instruments (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.

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 trade data stored in this subsystem occurs through one of two web applications: (1) ICE HSI and CBP users are granted access to all U.S. and foreign trade data via an internal DHS FALCON-DARTTS web application that resides within the DHS/ICE network, and (2) foreign users are granted access to select trade datasets via a different web application that resides within a protected infrastructure space between the DHS Internet perimeter and the DHS/ICE network. Foreign users can access only trade data about individuals or institutions with status in their country and 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 commercial off the shelf (COTS) software to assist 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, link analysis, and charting and graphing tools using proprietary statistical algorithms. 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 researching 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 alone 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 sources discussed below via CD-ROM, external storage devices, or electronic data transfers. Agencies that provide FALCON-DARTTS with trade data collect any PII directly from individuals or enterprises completing import-export electronic or paper forms. 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. 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 suspicious and HSI will coordinate joint investigations on those specific trade records. HSI may also open its own investigation.

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 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 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 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 CMAAs, MOUs, or other similar agreements. Certain countries provide trade data 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, the securities and futures industry, and casinos and card clubs); reports related to coins and currency received in 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 a 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 during 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.

ICE receives law enforcement records from the U.S. Department of the Treasury, Office of Foreign Assets Control's 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 are being conducted with a specially designated individual or entity, 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 data stored within the FALCON general data storage environment, eliminating the need for an additional copy. FALCON-DARTTS analysis of TECS subject records allows ICE HSI users to determine quickly if an entity 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 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. This information 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 use of FALCON-DARTTS, domestic HSI field offices and foreign attaché offices can initiate and enhance criminal investigations related to trade-based money laundering, trade fraud, and other financial crimes.

The FALCON-DARTTS system is helpful as an investigative tool in numerous HSI criminal investigations.

5. Laws and Regulations

DHS is authorized to collect information analyzed by FALCON-DARTTS pursuant to 19 U.S.C. §§ 1415, 1484 and 31 U.S.C. § 5316. ICE HSI has jurisdiction and authority to investigate violations involving importation or exportation of merchandise into or out of the United States. Information analyzed by FALCON-DARTTS supports HSI's investigations into numerous violations, including smuggling pursuant to 18 U.S.C. §§ 541, 542, 545, and 554 and money laundering pursuant to 18 U.S.C. § 1956. DHS is authorized to maintain documentation of these activities pursuant to 19 U.S.C. § 1415 (Mandatory Advance Electronic Information for Cargo and Other Improved Customs Reporting Procedures) 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, the Trade Secrets Act, and Bank Secrecy Act.

6. Privacy Impact and Privacy Protections

ICE does not use FALCON-DARTTS to make unevaluated decisions about individuals; FALCON-DARTTS is used solely as an analytical tool to identify anomalies. It is incumbent upon the HSI investigator to further investigate reasons for an anomaly. HSI investigators gather additional facts, verify accuracy of FALCON-DARTTS data, and use their judgment and experience to determine if an anomaly is suspicious and warrants further investigation for potential criminal violations. HSI investigators are required to obtain and verify original source data from the agency that collected the information to prevent inaccuracies 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. 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.

All raw data analyzed by FALCON-DARTTS is obtained from other governmental organizations that collect data under specific statutory authority. Therefore, FALCON-DARTTS relies on systems and/or programs performing original collection to provide accurate data. Most raw data used by FALCON-DARTTS is presumed accurate because the data was collected directly from an individual or entity. Due to the law enforcement context in which FALCON-DARTTS is used, however, there are often significant impediments to directly verifying information accuracy with the individual about whom specific information pertains. If errors in raw data are discovered by FALCON-DARTTS users, the FALCON-DARTTS system owner 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 pertinent to the analysis project. In the event uploaded data is later identified as inaccurate, it is the responsibility of the user to remove those records from the system and re-upload 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 appropriate changes to 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 access controls, user auditing, and accountability functions described in the FALCON-SA PIA. For example, user access controls allow data access restrictions at the record level, meaning only datasets authorized for a user-specific profile are visible and accessible by that user. Audit capabilities log user activities in a user activity report, which is used to identify users who are using the system improperly.

In addition to 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 is required to track, for each query, the identity of the user, time, and nature of the query, as well as the Bank Secrecy Act information viewed.

System access is granted only to ICE HSI, CBP, and foreign government personnel who require access to the functionality and data available in FALCON-DARTTS and its trade data subsystem in the performance of their official duties. Access is granted on a case-by-case basis by the FALCON-DARTTS Administrator designated by the HSI TTU Unit Chief. User roles are regularly reviewed by a FALCON-DARTTS HSI supervisor to ensure users have appropriate access and users who no longer require access are removed from the access list. All individuals 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. ICE 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 because 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 are retained for ten years per the above-mentioned legacy DARTTS records schedule. Some data used by FALCON-DARTTS is already maintained in the FALCON general data storage environment and is 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. ATLAS

2021 Program Update

There are no significant updates during this report period.

USCIS published a CIV PIA in February 2019, to address CIV privacy capabilities and privacy risks. The PIA describes enhanced screening capabilities to include additions to CIV updates within the ATLAS system.[79] 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.

ATLAS, not an acronym, is a U.S. Citizenship and Immigration Services screening and vetting platform which 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 of potential concerns to the USCIS Fraud Detection and National Security Directorate's (FDNS) investigative case management system, FDNS Data System (FDNS-DS), for review and administrative investigation.

1. Program Description

Every year, USCIS receives millions of 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 benefits or services, is to conduct screenings (i.e., background, identity, and security checks) on individuals who file requests for immigration benefits or action with the agency. USCIS/FDNS uses its investigative case management system, FDNS-DS 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.

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 ATLAS to automate 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 information provided by an individual or obtained through 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. USCIS published an ATLAS PIA in October 2020 to identify

[79] In 2014, FDNS developed 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.

ATLAS capabilities and address any privacy risks. Further USCIS updated the ATLAS PIA in May 2021 to include an Appendix outlining the ATLAS system connections and data sources for screening.

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

i. Allows preemptive notification to FDNS Officers of cases presenting suspected fraud, public safety, and/or national security concerns before adjudicators begin reviewing applications and provide updates on existing applicant filings through continuous vetting and monitoring;
ii. Increases consistency and timeliness for background and security check operations;
iii. Ensures consistent processes 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 benefit and request type. In general, USCIS conducts background checks to obtain relevant information to render appropriate adjudicative decision with respect to the benefit or service sought. USCIS also conducts identity checks to confirm an individual's identity and combat potential fraud, and security checks to identify potential threats to public safety or national security. Standard checks may include biometric, fingerprint-based checks such as the FBI Fingerprint Check; DHS's IDENT Fingerprint Check; and Department of Defense Automated Biometric Identification System (ABIS) Fingerprint Check; as well as biographic, name-based checks such as the FBI Name Check and TECS Name Check.

USCIS uses several systems to support requisite background, identity, and security checks, described in detail in various USCIS PIAs. As mentioned in those PIAs, USCIS adjudications staff must query multiple systems, in some cases manually. ATLAS greatly reduces the need to independently query each system, thereby streamlining screening and limiting privacy risks associated with using multiple systems. ATLAS interfaces with other systems to automate system checks and promotes consistent identification, storage, retrieval, and analysis of screening results to enable USCIS to detect and investigate fraud, public safety, and national security concerns more efficiently and effectively.

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

A. An individual presents themself 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 benefit request submission form submissions and from biographic and biometric-based checks listed above. This information is screened through ATLAS's rules engine, producing SGNs to automate the process of referring cases to FDNS for review. A specially trained FDNS Officer conducts a manual review of the SGN for validity and determines whether it is "actionable" or "inactionable," and, if "actionable," triages the notification for further action. If a notification is "actionable," it enters the formal FDNS-DS case management process. A SGN"inactionable" notification may be closed without further action. Notification itself is not considered derogatory. SGNs help FDNS Officers detect potential concerns in the immigration benefit request process, to demonstrate the fidelity of the individual's biographic and biometric information, and more efficiently identify discrepancies.

If FDNS determines an administrative investigation is necessary, FDNS conducts further checks to verify information prior to referring the case to an adjudicating officer to reach a 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 filing for immigration and naturalization benefits who may potentially engage in fraudulent behavior or who may pose a risk to public safety or national security. During screening, ATLAS analyzes results of biographic and biometric checks and applies rules against data received from multiple systems. ATLAS assists with confirming individuals' identities where individuals are potentially known by more than one identity. Confirmation is done by comparing identity information provided against identity information resident in other systems used in the security verification process. For example, ATLAS can determine if an individual applied for benefits using multiple biographic identities or aliases by matching fingerprints to various identities. Results of this analysis may be produced and sent to FDNS-DS in the form of a SGN.

ATLAS's 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 notification. 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 a SGN within FDNS-DS.

- U.S. Citizenship and Immigration Services (USCIS) Systems: Screening for CAMINO; Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR); USCIS Electronic Immigration System (ELIS) ; TECS by ELIS to facilitate checks by Computer Linked Application Information Management System (CLAIMS 3); GLOBAL; RAILS to retrieve the physical

locations of A-files; and Customer Profile Management System (CPMS) to retrieve data associated with biographic and biometric screening.

- Other U.S. Department of Homeland Security component System Interfaces: IDENT to retrieve data associated with biometric screening; CBP's TECS system, system via the CBP TECS Screening Service platform, to perform screening, including checks against the FBI NCIC; and CBP's ATS.

Additionally, FDNS Officers may manually query several internal and/or external databases or systems to obtain information to a case in FDNS-DS, such as:

- Other DHS Component Systems Accessed (Manually): AFI; ADIS; SEVIS; and ENFORCE Alien Removal Module;

- External Sources Accessed (Manually): Department of Labor; DoS; Department of Defense; Social Security Administration Electronic Verification of Vital Events (EVVE); Federal Aviation Administration websites; intelligence and law enforcement communities sources; state and local government agencies' sources; local, county, and state police information networks; state motor vehicle administration databases and websites; driver license retrieval websites; state bar association data; state comptroller data; state probation/parole boards or offices data; county appraisal districts data; 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."[80]

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. ATLAS is capable of automatically screening biometric and biographic information at intake, resolving identities when individuals use aliases. Between FY2020 and FY2021, ATLAS experienced a 25.6 percent growth in automated biographic and biometric screenings. In FY2021, ATLAS performed over 72.9 million combined biographic and biometric screenings on applicant information through law enforcement and other federal databases. SGNs generated in Fiscal Year 2021 resulted in over

[80] 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.

4,500 new immigration benefit fraud cases, over 375 new public safety cases, and over 750 new national security cases.

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 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 section 101(a)(17) of the INA); and (2) to investigate alleged civil and criminal violations of the immigration laws, including but not limited to, alleged fraud with respect to applications or determinations within USCIS, and make recommendations for prosecutions, or other appropriate action when deemed advisable.

USCIS has a statutory obligation to ensure applicants and/or beneficiaries are admissible in accordance with section 245(a)(2) of the INA. Section 245(a)(2) requires an alien must be admissible to the United States to adjust status to that of a lawful permanent resident.

Section 212 of the INA lists categories of inadmissible aliens. For example, an applicant may be found inadmissible if convicted of (or admit to having committed) an offense that constitutes 'crimes involving moral turpitude,' or has engaged in or is suspected of engaging in terrorist activities. Similarly, section 237 of the INA 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 or security and related grounds.

6. Privacy Impact and Privacy Protections

FDNS is committed to identifying threats to national security and public safety and combating immigration benefit fraud, while respecting individuals' privacy and promoting transparency of FDNS operations. In May 2016, FDNS updated and re-issued its PIA for the FDNS-DS system,[81] to provide public notice of the development of ATLAS, and to provide transparency into ATLAS's planned core capabilities. ATLAS was designed to allow FDNS to optimize processing of information purposes as outlined in the INA, while minimizing privacy risks. USCIS published an ATLAS PIA[82] in October 2020 to identify ATLAS capabilities and address and mitigate privacy risks. Further, USCIS updated the ATLAS PIA in May 2021, to include an Appendix outlining the ATLAS system connections and data sources for screening.

FDNS has responsibility to maintain accurate data because the information it collects could be used

[81] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* https://www.dhs.gov/privacy.
[82] *See* DHS/USCIS/PIA-084 ATLAS, October 2020, *available at* https://www.dhs.gov/publication/dhsuscispia-084-atlas.

in support of adjudicative decisions or criminal investigations undertaken by law enforcement partners. FDNS Officers rely on multiple sources to confirm data veracity and, if discrepancies are uncovered, take necessary steps to correct inaccuracies. This includes comparing information obtained during screening and administrative investigation processes with information provided directly by an 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. If FDNS Officers learn information contained within other systems is inaccurate, Officers notify appropriate USCIS personnel or the federal agency owning the data.

ATLAS does not collect information directly from individuals. Rather, ATLAS receives information from an individual's form submission and from associated biographic and biometric-based background checks, which include information from other DHS and USCIS systems. Immigration regulations (8 C.F.R. § 103.2(b)(16)) require individuals be advised of 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 or written responses to a Request for Evidence or a Notice of Intent to Deny NOID.

ATLAS's rules-based screening approach is tailored to provide information to FDNS Officers relevant to potential fraud, public safety, and national security threats. The issuance of a SGN does not indicate derogatory information about the individual. The notification process also provides for a layer of human review to confirm the notifications are actionable prior to routing them for further case management activity. FDNS continually monitors and refines rules based on appropriate metrics and to provide a focused scope of information for the FDNS Officers to review. 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 manual review of individual form submissions.

FDNS-DS maintains strict access controls so that only FDNS-DS users with a role in investigating cases for potential fraud, public safety, or national security concerns have access to raw data retrieved as part of the screening process. ATLAS interfaces with other systems to help streamline the review processes. Its capabilities are designed to assist FDNS Officers with 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 make a determination on the benefit or request sought.

Multiple layers of privacy and legal review are built into FDNS's processes, to reduce the risk of new data being incorporated into FDNS-DS that has not been reviewed for privacy and legal issues. 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 applicable exemptions, USCIS reviews all requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect national or homeland security of the United States or activities related to any investigatory material contained within the system, applicable exemptions may be waived at the discretion of USCIS, and in accordance with procedures and points of contact published in the applicable SORNs.

E. Global Command and Control System – Joint

2021 Program Update

There are no significant updates during this report period.

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 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, and to USCG's Unclassified Common Operating Picture (UCOP), to supplement the USCG's classified Common Operating Picture.

GCCS-J is a critical component of the Common Operating Picture that 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 provided in an annex to the report.

2. Technology and Methodology

GCCS-J is a commercial off the shelf product specifically built to perform a detailed view of a respective area of responsibility on both a strategic and tactical level.

3. Data Sources

On an operator-to-operator basis, GCCS-J data sources are used for tracking 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 Operating Picture and provides decision makers a detailed view of their respective area of responsibility either on a strategic or tactical level. 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 impacts 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 use of GCCS-J by providing roles, responsibilities, ownership, and accountability in use of the system. In addition, USCG entered 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; no additional privacy compliance documentation is required.

F. Unclassified Common Operating Picture (UCOP)

2021 Program Update

There are no significant updates during this report period.

1. Program Description

The USCG's UCOP consumes and disseminates unclassified products that aid Maritime Domain Awareness, 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 Common Operating Picture.

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 Office of Law Enforcement to use 21st century technologies to monitor compliance, track violators, and provide substantial evidence for prosecution while maintaining the integrity of individual fisherman's effort.

The system currently focuses data mining capabilities to allow USCG personnel in the Office of Law Enforcement to monitor and perform data analysis intended to identify suspicious anomalies that could indicate violations of laws that USCG enforces. 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 provided in an annex to the report.

2. Technology and Methodology

USCG UCOP and the Vessel Monitoring System (VMS), owned by NOAA, require interconnection between the two systems for the express purpose of exchanging data. This is authorized in accordance with the Interconnection Security Agreement (ISA) and MOU between USCG and NOAA. USCG Office of Law Enforcement uses 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 Common Operating Picture. This consolidation allows users to make informed decisions using the Tactical Decision Aids (TDAs) 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 attribute data about a vessel available to users and allows users to update/edit attribute information 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 the 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

UCOP provides dynamic vessel track data to unclassified and classified portrayal systems for the purpose of improved Maritime Domain Awareness, Intelligence Analysis, and resource allocation. In FY2021, data provided was used for life saving, human trafficking, drug interdiction, marine protection, and pollution cases.

5. Laws and Regulations

The Magnuson-Stevens Conservation and Management Act[83] authorizes collection of reliable data essential to the effective conservation, management, and scientific understanding of the fishery resources of the United States.[84] Data is collected for implementation of a standardized fishing vessel registration and information management system[85] which houses identification data for fishing vessels and basic fishery performance data.[86] Data processed between the USCG UCOP and NOAA VMS systems are categorized as Sensitive but Unclassified.

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 the system to identify vessels or aircraft. UCOP collects the MMSI number but does not link PII such as vessel owner name, email 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 a Memorandum, which clarified the responsibilities of the USCG to receive non-disclosure agreements prior to further internal or external sharing of NOAA VMS tracks.[87] On September 21, 2021, UCOP underwent a PTA to assess a need for additional Privacy compliance documentation; no additional documentation is required. Additionally, UCOP developed a System Privacy Plan (SPP) based upon a system review, documentation, DHS regulations/guidance, and interviews with information system and privacy personnel.

The UCOP is the only authorized path for Vessel Monitoring System data from NOAA to USCG. The NOAA feed to UCOP is a truncated version of the NOAA Office of Law Enforcement Vessel Monitoring System data, which is limited to position, location, and identification. The MOU between the USCG and NOAA, dated May 10, 2017, establishes data requirement exchanges between organizations. The MOU addresses communications, security incidents, disasters, and other contingencies.

The ISA between the USCG and NOAA, dated October 6, 2016, establishes technical requirements

[83] 16 U.S.C. § 1801 et seq.
[84] 16 U.S.C. § 1801(a)(8).
[85] 16 U.S.C. § 1881.
[86] *Id*.
[87] COMDT (CG-7612), 5510 dated June 26, 2018.

of interconnected IT systems. 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 Vessel Monitoring System owned by NOAA. The USCG requires use of NOAA Vessel Monitoring System, as a transport system for querying Vessel Monitoring System data in the NOAA database. As a matter of Coast Guard policy, and in consultation with NOAA Fisheries, Vessel Monitoring System, data is shared by NOAA Fisheries with the USCG for the specific purposes of Fisheries Law Enforcement and Search and Rescue.

Both organizations ensure adequate system access controls are in place and maintained on all components connected to the systems. Buildings that house the NOAA and UCOP servers are occupied by NOAA employees or Coast Guard personnel and are not open to the public. These structures are either part of NOAA federal buildings or located on Coast Guard bases.

Both parties ensure 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 persons with significant security responsibilities for the systems receive annual role-based training covering their specific areas of responsibility.

IV. Conclusions

Congress authorized the Department to engage in data mining in furtherance of the DHS mission while protecting privacy. The DHS Privacy Office is pleased to provide this fifteenth comprehensive report to Congress on DHS data mining activities, and remains vigilant in its oversight of these and other Department programs and systems.

V. Appendix

Acronym List	
ABIS	Department of Defense Automated Biometric Identification System
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-UPAX	Automated Targeting System—Unified Passenger Module
BCI	Border Crossing Information
CBP	U.S. Customs and Border Protection
CCD	Consolidated Consular Database
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
EID	Enforcement Integrated Database – ENFORCE Suite of Software Applications (i.e., ENFORCE Alien Removal Module or EID Arrest GUI for Law Enforcement (EAGLE)) Access EID data
EARM	ENFORCE Alien Removal Module

Acronym List	
ENFORCE	Not an Acronym - 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
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
IT	Information Technology
MDA	Maritime Domain Awareness
MOU	Memorandum of Understanding
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-CD	National Targeting Center-Cargo Division
OBIM	Office of Biometric Identity Management
OLE	Office of Law Enforcement
OMB	Office of Management and Budget
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PLI	Position, Location, Identification
PNR	Passenger Name Record

Acronym List	
PTA	Privacy Threshold Analysis
RFI	Request for Information
SAFE Port Act	Security and Accountability for Every Port Act
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
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