Data Mining for National Security:

U.S. Government Programs

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

This book provides an overview of data mining activities of the U.S. Government that focus on national security. The purpose is to preserve and disseminate that documentation. The editor is not attempting to copyright public documents.

Data mining enables corporations and government agencies to analyze massive volumes of data quickly and relatively inexpensively. The use of this type of information retrieval has been driven by the exponential growth in the volumes and availability of information collected by the public and private sectors, as well as by advances in computing and data storage capabilities. In response to these trends, generic data mining tools are increasingly available for—or built into—major commercial database applications.

There is no universally agreed-upon definition for the term "data mining." Some definitions of the term are quite broad. For example, the Technology and Privacy Advisory Committee ("TAPAC") of the Department of Defense defined data mining as: Searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.

Authors of other reports use narrower definitions. For example, the Congressional Research Service ("CRS") defines data mining as follows: Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees). Consequently, data mining consists of more than collecting and managing data, it also includes analysis and prediction.

The General Accountability Office (GAO) defines data mining as the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results. We based this definition on the most commonly used terms found in a survey of the technical literature. In the GAO initial survey of chief information officers, these officials found the definition sufficient to identify agency data mining efforts.

Federal agencies are using data mining for a variety of purposes, ranging from improving service or performance to analyzing and detecting terrorist patterns and activities. The GAO survey of 128 federal departments and agencies on their use of data mining shows that 52 agencies are using or are planning to use data mining. These departments and agencies reported 199 data mining efforts, of which 68 were planned and 131 were operational. The most common uses of data mining efforts were described by agencies

- as improving service or performance;
- detecting fraud, waste, and abuse;
- analyzing scientific and research information;
- managing human resources;
- detecting criminal activities or patterns; and

- analyzing intelligence and detecting terrorist activities

The Department of Defense reported having the largest number of data mining efforts aimed at improving service or performance and at managing human resources. Defense was also the most frequent user of efforts aimed at analyzing intelligence and detecting terrorist activities, followed by the Departments of Homeland Security, Justice, and Education.

In addition, out of all 199 data mining efforts identified, 122 used personal information. For these efforts, the primary purposes were detecting fraud, waste, and abuse; detecting criminal activities or patterns; analyzing intelligence and detecting terrorist activities; and increasing tax compliance.
(Link http://www.gao.gov/new.items/d04548.pdf)

Department of Homeland Security

The Homeland Security Act of 2002 expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission. DHS exercises this authority with respect to the programs discussed in the Department of Homeland Security Privacy Office 2015 Data Mining Report to Congress February 2016 report, all of which the DHS Chief Privacy Officer has reviewed for their potential impact on privacy. This section presents excerpts from the 2015 report.

While each program described below engages to some extent in data mining, no decisions about individuals are made based solely on data mining results. In all cases, DHS employees analyze the results of data mining, and then apply their own judgment and expertise to bear in making determinations about individuals initially identified through data mining activities. The DHS Privacy Office has worked closely with each of these programs to ensure that required privacy compliance documentation is current, that personnel receive appropriate privacy training, and that privacy protections have been implemented.

Program Updates
In the 2014 DHS Data Mining Report, the DHS Privacy Office discussed the following Departmental programs that engage in data mining:

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

Automated Targeting System (ATS) 2015 Program Update

Non-Immigrant and Immigrant Visa Applications
As described in the 2012 ATS PIA, ATS-P (now known as ATS-UPAX) is used to vet non-immigrant visa applications for the U.S. Department of State (DoS). In January 2013, CBP and DoS began pre-adjudication investigative screening and vetting for immigrant visas. DoS sends online visa application data to ATS-UPAX for pre-adjudication vetting. ATS-UPAX vets the visa application and provides a response to the DoS's Consular Consolidated Database (CCD) indicating whether DHS has identified derogatory information about the individual. Applications of individuals for whom derogatory information is identified through ATS-UPAX are either vetted directly in ATS-UPAX, if a disposition can be determined without further research, or

additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net) case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD. The Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA) (Pub. L. 107-173), 8 U.S.C. § 1721, authorizes the use of ATS-UPAX for screening non-immigrant and immigrant visas.

Overstay Vetting

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

As with the Phase 2 Pilot, discussed in DHS's 2013 and 2014 Data Mining Reports, Phase 3 also uses foreign national overstay data obtained through system processing in ATS-UPAX and ADIS to identify certain individuals who have remained in the United States beyond their authorized period of admission (overstays) and who may present a heightened security risk. In January 2014, ADIS transitioned from the Office of Biometric Identity Management (OBIM) in the DHS National Protection and Programs Directorate to CBP. The goal of the Overstay Vetting effort is to allow ICE to deploy its investigative resources efficiently to locate high-risk overstays and initiate criminal investigations or removal proceedings against those individuals. CBP uses biographical information on identified and possible overstays in ADIS to be run in ATS-UPAX against risk-based rules based on information derived from past investigations and intelligence. CBP provides results of these analyses from ADIS to ICE for further processing. These activities are covered by PIAs for ATS, the US-VISIT Technical Reconciliation Analysis Classification System, and Overstay Vetting.

Trusted Traveler Vetting

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

On May 4, 2015, ATS Trusted Traveler Vetting Program capabilities were deployed to a CBP Vetting Center. ATS provides improved vetting algorithms, which are designed to assist in identifying more refined matches to derogatory records. The results of the vetting analysis provide a consolidated view of the applicant's information, derogatory matches, as well as other system checks. In November 2015, the ATS Trusted Traveler Vetting capabilities included a new

grouping of Trusted Traveler applications that are marked as candidates for Auto-Conditional approval if certain conditions are met in the automated risk assessment process. At the time of this report, the information derived from these new capabilities is being used for testing and evaluation purposes only; these applications are not currently auto-conditionally approved. This testing and evaluation period will provide valuable data to determine if, or when, the automated process will occur. Once this process is reviewed and refined to sufficiently meet CBP requirements, ATS-UPAX will begin to auto-conditionally approve Trusted Traveler applicants, who will be referred directly to the Enrollment Centers for interview. This process is expected to reduce the workload for the CBP Vetting Center. Full transition to vetting of Trusted Traveler applicants in the ATS platform is expected by the second quarter of FY2016.

Special ATS Programs

ATS Enhancements to Watchkeeper System
Watchkeeper is the United States Coast Guard's (USCG) information sharing and management USCG enhanced Watchkeeper by integrating the ATS-N and ATS-UPAX modules, discussed below, as tools to conduct pre-arrival screening and vetting of vessel cargo, crew, and passengers. This enhanced program became operational in November 2014. The ATS-enhanced Watchkeeper provides near real-time data for Captains of the Port (COTP) to better evaluate threats and deploy resources through the active collection of incoming vessel information. With a more detailed picture of the risk profile that a vessel presents, COTPs can make appropriate, informed decisions well ahead of the vessel's arrival in port.

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

Following the success of Phase 1 of this program, TSA and CBP sought to move beyond their success in resolving vetting inconsistencies of watchlisted passengers to expand their collective view of air domain security. Phase 2 of the TSA/CBP COP program began in September 2014, and sought to expand the success of Phase 1 by including additional information in the common

dashboard display for both TSA and CBP. This information includes: passengers who are confirmed or possible matches to the watchlists on international flights of covered U.S. aircraft operators; passengers on domestic flights who are confirmed matches to the DNBL or TSDB also uses ATS to identify other potential violations of U.S. laws that CBP enforces at the border under its authorities. ATS allows CBP officers charged with enforcing U.S. law and preventing terrorism and other crimes to focus their efforts on the travelers, conveyances, and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Traveler, conveyance, and shipment data are processed through ATS and are subject to a real-time, rules-based evaluation.

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

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

The U.S. Customs Service, a legacy organization of CBP, traditionally employed computerized tools to target potentially high-risk cargo entering, exiting, and transiting the United States, or persons who may be importing or exporting merchandise in violation of United States law. ATS was originally designed as a rules-based program to identify such cargo and did not apply to travelers. ATS-N and ATS-AT44 became operational in 1997. ATS-P (now referred to as ATS-UPAX) became operational in 1999 and is now even more critical to CBP's mission. ATS-UPAX allows CBP officers to determine whether a variety of potential risk indicators exist for travelers or their itineraries that may warrant additional scrutiny.

ATS-UPAX maintains Passenger Name Record (PNR) data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from certain air carriers in 1997. Currently, CBP collects this information to the extent it is collected by carriers in connection with a flight into or out of the United States, as part of CBP's border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).

ATS ingests various data in real-time from the following DHS and CBP systems: the Automated Commercial System (ACS), the Automated Manifest System (AMS), the Advance Passenger Information System (APIS), the Automated Export System (AES), the Automated Commercial Environment (ACE), the Electronic System for Travel Authorization (ESTA), the TECS maintains information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC) TSDB and provides access to the Department of Justice's (DOJ) National Crime Information Center (NCIC), which contains information about individuals with outstanding wants and warrants, and to Nlets (formerly the National Law Enforcement Telecommunications System), a clearinghouse for state wants and warrants as well as information from state Departments of Motor Vehicles (DMV).

ATS collects PNR data directly from air carriers. ATS also collects data from certain airlines, air cargo consolidators (freight forwarders), and express consignment services in ATS-N. ATS accesses data from these sources, which collectively include: electronically filed bills of lading (i.e., forms provided by carriers to confirm the receipt and transportation of on-boarded cargo to U.S. ports), entries, and entry summaries for cargo imports; Electronic Export Information (EEI) (formerly referred to as Shippers' Export Declarations) submitted to AES and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land border crossing and referral records for vehicles crossing the border; airline reservation data; non-immigrant entry records; records from secondary referrals, incident logs, and suspect and violator indices; seizures; and information from the TSDB and other government databases regarding individuals with outstanding wants and warrants and other high-risk entities.

The functionality of ATS-AT was modernized when the AES system was re-engineered and deployed by CBP. AES aids CBP officers in identifying export shipments that pose a high risk of containing goods requiring specific export licenses, illegal narcotics, smuggled currency, stolen vehicles or other contraband, or exports that may otherwise violate U.S. law. This targeting functionality in AES sorts EEI data, compares it to a set of rules, and evaluates it in a comprehensive fashion. This information assists CBP officers in targeting or identifying exports that pose potential aviation safety and security risks (e.g., hazardous materials) or may be otherwise exported in violation of U.S. law.

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

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

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

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.

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

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

Data Sources

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

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

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

Based on the results of testing and operations in the field, ATS-N and ATS-AT have proven to be effective means of identifying suspicious cargo that requires further investigation by CBP officers. The results of ATS-N and ATS-AT analyses identifying cargo as suspicious have been regularly corroborated by physical searches of the identified cargo.

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

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

ATS-UPAX continues to rely on the risk-based rules that are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local

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

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

TS-UPAX uses available information from the following databases to assist in the development of the risk-based rules discussed above: APIS; NIIS, which contains all Form I-94 Notice of Arrival/Departure records and actual ESTA arrivals/departures; ESTA, which contains pre-arrival information for persons seeking authorization to travel under the Visa Waiver Program (VWP)59; the DHS Suspect and Violator Indices (SAVI); and the DoS visa databases. ATS-UPAX also relies upon PNR information from air carriers, BCI crossing data, seizure data, Report of International Transportation of Currency or Monetary Instrument Report (CMIR) data, and information from the TSDB and TECS.

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

In the past year, ATS-UPAX has identified, through lookouts and/or risk-based rule sets, individuals who were confirmed matches to the TSDB and caused action to be taken to subject them to further inspection or, in some cases, made recommendations to carriers not to board such persons. ATS-UPAX matches have also enabled CBP officers and foreign law enforcement partners to disrupt and apprehend persons engaged in human trafficking and drug smuggling operations. For example, CBP officers working at the NTC using ATS-UPAX identified a subject who was involved in terrorism financing. Based on the research conducted by the NTC, the subject was nominated to the TSDB and the individual's visa was revoked by the DoS. Subsequently, the subject attempted to travel to the United States, and CBP contacted the air carrier and advised that the subject would likely be found inadmissable to the United States if permitted to travel. The subject was denied boarding by the air carrier. In another instance, CBP, working at the NTC in conjunction with a United States Marshals Service (USMS) Liaison, identified a U.S. Citizen who was living abroad and was a USMS Top 15 fugitive for sexual abuse of minors. Using ATS-UPAX, CBP was able to provide information to USMS to assist in locating the fugitive, which subsequently led to his arrest.

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

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

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

ATS-L provides information to its users in real time, permitting an officer to assess his or her response to the crossing vehicle or person prior to initiating the border crossing process. The automated nature of ATS-L is a significant benefit to officer safety by alerting officers of potential threats prior to a vehicle's arrival at the point of inspection. It also greatly increases the

efficiency and effectiveness of the officer's otherwise manual and labor-intensive work checking individual databases, thereby facilitating the more efficient movement of vehicles, their occupants, and pedestrians, while safeguarding the border and the security of the United States. CBP officers and agents use the information generated by ATS-L to aid their decision-making about risk associated with vehicles, their occupants, and pedestrians. As discussed above, ATS includes real-time updates of information from ATS source systems to ensure that CBP officers and agents are acting upon the most up to date information. For example, in October 2015, ATS-L alerted CBP Officers to a vehicle bearing California plates and the vehicle occupants, two United States citizens, were referred to secondary for inspection. During secondary inspection, a canine alerted to the undercarriage of the vehicle. An inspection of the vehicle found tampering to the sending unit underneath the back passenger's seat. The cover was removed which revealed packages in the gas tank. A field test showed the substance in the packages was methamphetamine. The driver was arrested for the importation of narcotics. A total of thirty-two (32) packages of methamphetamine weighing 36.61 lbs. were seized.

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

ATS Privacy Impacts and Privacy Protections

The DHS Privacy Office has worked closely with CBP to ensure that ATS satisfies the privacy compliance requirements for operation. As noted above, CBP completed an updated PIA for ATS on September 16, 2014, and updated the SORN for ATS in June 2012. CBP, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel conduct joint quarterly reviews of the risk-based targeting rules used in ATS to ensure that the rules are appropriate, relevant, and effective and assess whether privacy and civil liberties protections are adequate and consistently implemented.

Authorized CBP officers and agents and personnel from ICE, TSA, USCG, and U.S. Citizenship and Immigration Services (USCIS) who are located at seaports, airports, land border ports, and operational centers around the world use ATS to support targeting-, inspection-, and enforcement-related requirements. ATS supports, but does not replace, the decision-making responsibility of CBP officers, agents, and analysts. Decisions made or actions taken regarding individuals are not based solely on the results of automated searches of data in the ATS system. Information obtained in such searches assists CBP officers and analysts in either refining their analysis or formulating queries to obtain additional information upon which to base decisions or actions regarding individuals crossing U.S. borders.

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

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

Analytical Framework for Intelligence (AFI) 2015 Program Update

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

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

AFI augments CBP's ability to gather and develop information about persons, events, and cargo of interest by creating an index of the relevant data in the existing operational systems and providing AFI analysts with different tools that assist in identifying non-obvious relationships. AFI allows analysts to generate finished intelligence products to better inform finished intelligence product users about why an individual or cargo may be of greater security interest

based on the targeting and derogatory information identified in or through CBP's existing data systems. CBP currently utilizes transaction-based systems such as TECS and ATS for targeting and inspections. AFI enhances the information from those systems by utilizing different analytical capabilities and tools that provide link analysis among data elements.

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

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

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

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

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

AFI also serves as a workspace that allows AFI analysts to create finished intelligence products, to maintain and track projects throughout their lifecycle from inception to finished intelligence product or from RFI to response, and to share finished intelligence products either within DHS or