Privacy Impact Assessment Update
for the

Automated Targeting System

December 2, 2008

Contact Point
Troy Miller
Office of Intelligence and Operations Coordination
U.S. Customs and Border Protection

(202) 344-1883

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This is an update to the previous Automated Targeting System (ATS) privacy impact assessment, dated August 3, 2007, in order to expand the scope of the data accessed for screening and targeting purposes to include additional importer and carrier requirements. In conjunction with this update, CBP is publishing an Interim Final Rule that amends the CBP regulations contained in 19 CFR Parts 4, 12, 18, 101, 103, 113, 122, 123, 141, 143, 149, 178, and 192 addressing the advanced electronic submission of information by importers and vessel carriers.

Introduction

ATS is an intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. As a decision support tool ATS compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP. In this way, ATS allows CBP officers charged with enforcing U.S. law and preventing terrorism and other crime 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 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 rule based evaluation.

ATS consists of six modules that provide selectivity and targeting capability to support CBP inspection and enforcement activities.

- ATS-Inbound – inbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Outbound – outbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Passenger (ATS-P) – travelers and conveyances (air, ship, and rail)
- ATS-Land (ATS-L) - private vehicles arriving by land
- ATS - International (ATS-I) - cargo targeting for CBP's collaboration with foreign customs authorities
- ATS-Trend Analysis and Analytical Selectivity Program, (ATS-TAP) (analytical module)

ATS uses information from CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies, and risk-based rules

developed by analysts to assess and identify high-risk cargo, conveyances, and travelers that may pose a greater risk of terrorist or criminal activity and therefore should be subject to further scrutiny or examination.

In order to improve CBP's ability to identify high-risk shipments so as to prevent smuggling and ensure cargo safety and security, and in fulfillment of the statutory mandate provided by section 203 of the Security and Accountability for Every Port Act of 2006 (Pub. L. 109-347, 120 Stat. 1884 (SAFE Port Act) and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002, CBP is amending its regulations to require importers and vessel carriers to submit additional information pertaining to cargo before the cargo is brought to the U.S by vessel. This PIA updates the original ATS PIA and addresses the expansion of the system's access to data to include this additional information.

Currently vessel carriers are required to submit advance cargo information for vessels, including a vessel's Cargo Declaration, to CBP via the Vessel Automated Manifest System (AMS) no later than 24 hours before the cargo is laden aboard a vessel at a foreign port. Importers of record are generally required to file entry information, including CBP Form 3461, with CBP within fifteen calendar days of the date of arrival of a shipment of merchandise at a United States port of entry. Additionally importers are required to file entry summary information, including CBP Form 7501, within ten working days of the entry of the merchandise. This entry and entry summary information is submitted to CBP electronically via the Automated Broker Interface (ABI) or by paper forms. Presently, the information in both AMS and ABI resides partly within the Automated Commercial System (ACS), CBP's legacy trade and commercial system, and partly within the Automated Commercial Environment (ACE), CBP's future trade and commercial system; the collection and maintaining of this information is covered by the ACS System of Records Notice.

Under the new regulations, CBP requires vessel carriers to submit two additional data elements – a Vessel Stow Plan (VSP) and Container Status Messages (CSM) regarding certain events relating to containers loaded on vessels destined for the United States. Additionally, importers are required to submit an Importer Security Filing (ISF) containing ten new data elements of which several (e.g., Manufacturer, Seller, Buyer, Ship to party, and Consolidator) may contain personally identifying information about an individual so identified. Collectively, this data is commonly referred to by the trade as "10 + 2" data. Inasmuch as the new carrier submissions – the Vessel Stow Plan and the Container Status Messages – do not contain any personally identifiable information, this PIA will focus on the Importer Security Filing (ISF) which may contain personally identifiable information.

Importer Security Filing

For cargo, other than foreign cargo remaining on board (FROB) a vessel or goods intended to move through the United States, the new regulations require ISF Importers, or their agents, to transmit an ISF to CBP generally no later than 24 hours before cargo is laden aboard vessels destined to the United States. The ISF must consist of the following ten elements, unless an element is specifically exempted: 1) Manufacturer (or supplier); 2) Seller; 3) Buyer; 4) Ship to party; 5) Container stuffing location; 6) Consolidator (stuffer); 7) Importer of record number/Foreign Trade Zone applicant identification number; 8) Consignee number(s); 9) Country of origin; and 10) Commodity HTSUS number.

Alternatively, for shipments consisting entirely of FROB and shipments consisting of goods intended to move through the United States, ISF Importers, or their agents, must submit the following five elements, unless an element is specifically exempted: 1) Booking party; 2) Foreign port of unlading; 3) Place of delivery; 4) Ship to party; and 5) Commodity HTSUS number. Because FROB is frequently laden based on a last-minute decision by the vessel carrier, the ISF for FROB is required any time prior to lading.

With regard to either type of shipment, the party filing the ISF is required to update the submission if, after the filing and before the goods arrived within the limits of a port in the United States, there are changes to the information or more accurate information becomes available. The ISF importer, or designated agent, must submit the ISF via a CBP-approved electronic data interchange system. At this time CBP-approved electronic data interchange systems are ABI and vessel AMS, both of which are modules of the Automated Commercial System (ACS). Once the ISF has been initially collected by ACS, the information is immediately transferred to the ATS-Inbound (ATS-Inbound) cargo module for screening and targeting. Following processing by ATS-Inbound, ISF data will be transmitted back to ACS to be maintained in accordance with its retention provisions. As a result of the screening and targeting in ATS-Inbound and consistent with the existing ATS SORN, links or pointers to specific transactions and aspects of those transactions, which have positive matches to rule sets in ATS-Inbound, and the corresponding risk assessment and score will be maintained in ATS-Inbound.

Reason for the PIA Update

In accordance with Section 222 of the Homeland Security Act of 2002, this PIA update is required by the amendment of CBP regulations that expand the amount of data being screened and targeted through ATS-Inbound to include the ten new data elements represented by the ISF, of which five of the data elements may include personally identifying information (e.g., a reference to a name and address).

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The new regulations mandate the collection of additional data elements relating to cargo, which may include personally identifying information. For every shipment of cargo other than FROB, and cargo moving through the United States, the ISF must contain the following data elements, unless exempted: the manufacturer (or supplier), seller (*i.e.*, full name and address or widely accepted business number such as a DUNS number), buyer (*i.e.*, full name and address), ship to party (full name and/or business name and address), container stuffing location, consolidator (stuffer), importer of record number/foreign trade zone applicant identification number, consignee number(s), country of origin and commodity Harmonized Tariff System of the United States (HTSUS) number. For every FROB shipment or shipment of cargo moving through the United States, the data elements required include: the booking party (*i.e.*, name and address), foreign port of unlading, place of delivery, ship to party and commodity HTSUS number.

These additional data elements are necessary to improve CBP's ability to identify high-risk shipments so as to prevent smuggling and ensure cargo safety and security, in fulfillment of the statutory mandate provided by section 203 of the Security and Accountability for Every (SAFE) Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002.

Uses of the System and the Information

There are no new uses of data currently being collected for ATS based on this update. As described in the previous PIA, the information that is screened and targeted through ATS-Inbound is used to support inspection, examination, and counter-terrorism related requirements of CBP's mission. Information relating to both the seller and buyer is included in this screening to ensure that all aspects of the transaction are evaluated.

Retention

Data retention for ATS is unchanged as a result of this update. As described in the previous PIA, information initially collected by ATS is used for entry, exit and in-transit screening and risk assessment purposes. Information in this system will be retained and disposed of in accordance with the records schedule approved by the National Archives and Records Administration. To the extent that data is accessed from other systems, that data, essentially a pointer or link to the data, is retained in accordance with the record retention requirements of those systems.

Notwithstanding the foregoing, information maintained only in ATS that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (*i.e.*, specific and credible threats, and flights, individuals and routes of concern, or other defined sets of

circumstances), will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Internal Sharing and Disclosure

There are no new data disclosures within CBP as a result of this update. As described in the previous PIA, the principle users of ATS data are within DHS, and include CBP Office of Field Operations (OFO), CBP Office of Intelligence and Operations Coordination (OIOC) (previously the CBP Office of Intelligence), CBP National Targeting Center (NTC), CBP Office of International Trade (OT), U.S. Immigration and Customs Enforcement (ICE), DHS Office of Intelligence and Analysis and the Transportation Security Administration. The information collected through ATS may be shared with component agencies within DHS on a need to know basis consistent with the component's mission. Access to ATS is role-based according to the mission of the component and the user's need to know.

External Sharing and Disclosure

There are no new data disclosures outside CBP as a result of this update. With regard to the information maintained in the ATS-Inbound cargo module, information sharing agreements for access outside of DHS to information regarding imported commodities exist with the U.S. Department of Agriculture (this access includes viewing of specific USDA risk assessments and rule sets), the U.S. Food and Drug Administration (FDA) (limited to personnel at the FDA Prior Notice Center) and the Canada Border Security Agency (CBSA).

Notice

No changes have been made to the notice. The use of the information is consistent with the existing system of records notice previously published in the Federal Register

Individual Access, Redress, and Correction

No changes have been made in individual access, redress and correction as a result of this update. Requests for access to personally identifiable information, contained in the Importer Security Filing maintained within ACS, that was provided regarding the requestor, by the requestor or by someone else on behalf of the requestor may be submitted to the Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511)

Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Technical Access and Security

No changes have been made to technical access and security as a result of this update.

Technology

No technology has changed as a result of this update.

Responsible Official

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of International Trade, Regulations and Rulings, U. S. Customs and Border Protection, (202) 325-0280.

Troy Miller, Director, Operational Analysis, Office of Intelligence and Operations Coordination, U.S. Customs and Border Protection, (202) 344-1883.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security