Privacy Impact Assessment
for the

Air Cargo Advance Screening (ACAS)

DHS/CBP/PIA-061

October 29, 2019

Contact Point
Dennis McKenzie
Deputy Executive Director
Manifest and Conveyance Security Division
(202) 344-1808

Reviewing Official
Jonathan Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) requires air-cargo and shipping companies to submit their electronic manifest information in advance to CBP under the Air Cargo Advance Screening (ACAS) program. This advance information improves CBP's ability to conduct risk assessments of incoming shipments in order to improve security and compliance with customs and other laws CBP enforces at the border. CBP is publishing this new Privacy Impact Assessment (PIA) to provide notice of the new mandatory requirements for ACAS participants, and to assess the privacy risks of its collection and use of personally identifiable information under this program.

Overview

In October 2010, terrorists placed concealed explosive devices in cargo onboard two aircraft destined to the United States. The terrorists intended the explosive devices to explode mid-air over the continental United States, which could have caused catastrophic damage to the aircraft, the passengers, crew, and persons and property on the ground.[1] While multiple foreign governments thwarted the attempted attack by working together to share intelligence and intercept the shipments before they detonated, the explosive devices flew aboard several flights prior to discovery. In order to deter and disrupt terrorist threats to U.S.-bound aircraft via air cargo, the Department of Homeland Security (DHS) must identify high-risk cargo prior to the aircraft's departure for the United States. CBP and the Transportation Security Administration (TSA)[2] are responsible for securing air cargo bound for the United States. CBP and TSA employ a layered security approach to secure inbound air cargo, including using various risk assessment methods to identify high-risk cargo and to mitigate any risks posed.

Legacy Air Cargo Screening Requirements

Pursuant to the Trade Act of 2002,[3] as amended, any inbound aircraft entering or traveling through the United States with commercial cargo aboard must electronically submit to CBP certain information concerning the incoming cargo. 19 CFR § 122.48a requires carriers to submit eighteen advance electronic manifest data elements to CBP four hours prior to arrival for long-haul flights,[4] but no later than the loading of an aircraft, or "wheels-up" for short-haul flights. CBP uses this information to screen inbound aircraft for potential high-risk shipments that might warrant additional scrutiny. The CBP National Targeting Center (NTC), staffed by both CBP and TSA analysts, generates requests for additional information and screening referrals based on this

[1] www.cbp.gov/newsroom/national-media-release/air-cargo-advance-screening.
[2] Outside of the ACAS program, TSA has other regulatory responsibilities and oversight in relation to aircraft screening requirements.
[3] Pub. L. 107–210, H.R. 3009, 116 Stat. 933, enacted August 6, 2002; 19 U.S.C. §§ 3803–3805.
[4] A long-haul flight is a flight over seven hours in length.

information. CBP and TSA staff review electronic messages[5] describing upcoming shipments in advance of cargo departure for the United States to identify any potential threats. In response, CBP returns an acknowledgement message to the submitter, as well as any holds on the shipment via CBP's Automated Targeting System (ATS).[6]

The timeframes under this regulatory framework did not provide CBP adequate time to perform targeted risk assessments on air cargo before the aircraft departed.[7] As a result, there was a risk that CBP would not be able to identify high-risk cargo until it was already en route. In an effort to reduce these risks and to improve its security assessment capabilities, CBP developed the Air Cargo Advance Screening (ACAS) pilot in 2010 to allow air transport participants (such as air-cargo carriers and shipping companies) to voluntarily provide CBP with a subset of the advance electronic manifest information earlier than regulations required. CBP determined that the pilot was successful and initiated the administrative rulemaking process to require advance filing for all airlines during the ACAS pilot, as having the data elements submitted to the NTC for targeting earlier enabled CBP to better identify high-risk cargo subject to additional screening.

2018 New ACAS Regulations

The ACAS Program went into effect on June 12, 2018, requiring the submission of advanced air-cargo information on shipments arriving in the United States from a foreign location. Previously a voluntary process in which many airlines already participated globally, the program requirements are now mandatory for airlines flying to the United States.

Accordingly, CBP issued new regulations in June 2018 that mandated the provision of this advance information. Under the new regulations, CBP requires ACAS data elements as early as practicable, but no later than prior to loading of the cargo onto the aircraft for all flights. The transmission of the required ACAS data to CBP (also known as the "ACAS filing") must take place through the existing CBP-approved electronic data interchange system in ATS. CBP may take appropriate enforcement action against ACAS filers who do not comply with the ACAS requirements.

ACAS Mandatory Data Elements

CBP collects and maintains ACAS information in ATS, which evaluates all cargo to identify high risk inbound cargo and conveyances for examinations. ATS uses risk-based rules and weight sets to analyze information from manifest, Importer Security Filing,[8] and entry data to prioritize shipments for review and generate targets by scoring each shipment. In some instances,

[5] Messages modeled on either existing Cargo-IMP format messages or CBP CAMIR-AIR.
[6] DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[7] Defined in 19 CFR § 122.48a(b).
[8] Before merchandise arriving by vessel can be imported into the United States, the importer, or its agent, must electronically submit certain advance cargo information to CBP in the form of an Importer Security Filing.

ATS automatically places shipments on hold (detained) when they score above a specified risk threshold based on ACAS data (and other information available to CBP). ATS screens commodity information on the manifest, Importer Security Filing, and entry data, and ATS also screens individuals identified in these data sources against lookouts and prior violations.

Receiving information early from ACAS through ATS allows CBP to conduct targeting and risk assessment in ATS of shipments prior to the loading of aircraft destined for the United States. Like the pilot, the ACAS program requires an eligible filer (as described below) to submit six of the eighteen existing advance electronic manifest data elements listed below (and enumerated in 19 C.F.R § 122.48a):

- Shipper name and address;[9]
- Consignee name and address;[10]
- Cargo description;[11]
- Total quantity (based on the smallest external packing unit);[12]
- Total weight of cargo;[13] and
- Air waybill number.[14]

In addition to the mandatory data elements listed above, filers have the option to provide the remainder of the manifest data either in advance, or under the timeframes set forth under previous regulations.[15]

In addition to mandating ACAS data, CBP's revisions to 19 CFR § 122.48a provided more accurate and complete definitions and added a new data element (the flight departure message, or FDM) to enable CBP to determine the timeliness of ACAS submissions.

ACAS Filers

Potential ACAS filers must do the following:

- Establish the communication protocol required by CBP for properly transmitting

[9] For consolidated shipments, the identity of the consolidator, express consignment, or other carrier, is sufficient for the master air waybill record. For non-consolidated shipments, the name of the foreign vendor, supplier, manufacturer, or other similar party is acceptable (and the address of the foreign vendor, etc., must be a foreign address); by contrast, the identity of a carrier, freight forwarder, or consolidator is not acceptable.
[10] Consignee name and address is the name and address of the party to whom the cargo will be delivered and is required regardless of the location of the party; this party need not be located at the arrival or destination port.
[11] Cargo description is a precise description of the cargo or the 6-digit Harmonized Tariff Schedule (HTS) number.
[12] For example, 2 pallets containing 50 pieces each would be considered 100, not 2.
[13] Total weight of cargo may be expressed in either pounds or kilograms.
[14] The air waybill number is the International Air Transport Association (IATA) standard 11-digit number.
[15] 19 CFR § 122.48a.

an ACAS filing through a CBP-approved electronic data interchange system;

- Possess the appropriate bond;
- Report all of the originator codes that will be used to file ACAS data; and
- Provide 24 hours/7 days a week contact information consisting of a telephone number and email address.

Inbound air carriers are required to file the ACAS data if no other eligible party elects to file.[16] However, CBP allows parties other than the inbound air carrier to file because, in some cases, these other parties have access to accurate ACAS data sooner. For effective targeting to occur prior to loading, it is essential that the most accurate ACAS data be filed at the earliest point possible in the supply chain. This approach is consistent with the Trade Act parameters that require CBP to obtain data from the party most likely to have direct knowledge of the data and to balance the impact on the flow of commerce with the impact on cargo safety and security.

Other eligible filers include: importers or customs brokers as identified by the Automated Broker Interface (ABI) filer code;[17] a Container Freight Station/de-consolidator[18] as identified by its Facilities Information and Resources Management System (FIRMS) code;[19] an Express Consignment Carrier Facility[20] as identified by its FIRMS code; or an air carrier as identified by its carrier International Air Transport Association (IATA) code[21] that arranged to have the inbound air carrier transport the cargo to the United States.

Foreign Indirect Air Carriers (FIACs) are generally ineligible to directly file the advance air-cargo data required under 19 CFR 122.48a. However, FIACs that are not eligible 19 CFR 122.48a filers are still eligible to transmit ACAS-only filings. CBP allowed FIACs to participate in the ACAS pilot because the house air waybill (HAWB) data (which is each shipment within a consolidated shipment) is generally available to the FIACs earlier than it is available to the inbound air carrier. The master air waybill (MAWB) is an air waybill that is generated by the inbound carrier for a consolidated shipment. CBP has concluded that the inclusion of FIACs in the ACAS pilot has resulted in CBP's receipt of the data earlier in some cases.

[16] ACAS information is filed by eligible parties as defined by 19 CFR § 122.48b(c).
[17] Automated Broker Interface (ABI) is an integral part of the Automated Commercial System (ACS) that permits qualified participants to file import data electronically with CBP. The ABI filer is identified by the ABI filer code.
[18] A Container Freight Station is a facility where freight shipments are consolidated or de-consolidated and staged between transport legs. A CFS is typically located in proximity to an ocean, port, or airport, where cargo containers are transported to and from.
[19] A FIRMS code is a four-digit alphanumeric identifier assigned by CBP to Container Freight Stations, Warehouse Deconsolidators, Foreign Trade Zones, Bonded Warehouses, or any other CBP bonded facility.
[20] Express Consignment Carrier Facility is a bonded warehouse that is able to handle express high-volume parcel flows into the United States.
[21] IATA Airline codes are two letter characters assigned by the International Air Transport Association to represent airlines around the world.

ACAS Referrals

After CBP conducts a risk assessment for the ACAS filing, it may issue two types of referrals: referrals for information, and referrals for screening.

- CBP may issue a *referral for information* if CBP cannot conduct a risk assessment of the cargo due to non-descriptive, inaccurate, or insufficient data. This may be due to typographical errors, vague cargo descriptions, and/or unverifiable data. For referrals for information, the party who filed the ACAS data must resolve the referral by providing CBP with the requested clarifying data. In a dual ACAS filing, the last party to file the ACAS data must address the referral. For instance, when the inbound air carrier retransmits an original ACAS filer's data in a dual filing situation and a referral for information is issued after this retransmission, the inbound air carrier is responsible for taking the necessary action to address the referral.
- CBP may issue a *referral for screening* if CBP deems the potential risk of the cargo high enough to warrant a security screening method beyond the baseline, in accordance with appropriate TSA-approved screening methods. The ACAS filer can perform the necessary screening provided it is a party recognized by TSA to perform screening. If operating under an approved amendment[22] to the security program, the measures specified in that amendment will apply whether it be a TSA National Cargo Security Program (NCSP) amendment or other amendment. If the filer chooses not to perform the screening or is not a party recognized by TSA to perform screening, the ACAS filer must notify the inbound air carrier of the referral for screening. Once the inbound air carrier is notified of the unresolved referral for screening, the inbound air carrier must perform the required screening, and/or provide the necessary information to CBP to resolve the referral for screening. The ultimate responsibility to resolve any outstanding referral for screening is placed on the inbound air carrier because that is the party with physical possession of the cargo prior to departure of the aircraft.

CBP will issue a Do-Not-Load (DNL) instruction if it determines, based on the risk assessment and other information, that the cargo may contain a potential bomb, improvised explosive device, or other material that may pose an immediate, lethal threat to the aircraft and/or its vicinity. All ACAS filers must provide a telephone number and email address that is monitored 24 hours/7 days a week in order for CBP to contact them to prevent the cargo from moving. All ACAS filers must respond and fully cooperate when a DNL instruction is issued.

[22] TSA has the flexibility to modify its air-cargo screening requirements as needed based on changing security environments, intelligence, and emergency situations through Emergency Amendments/Security Directives (EAs/SDs).

Sample Scenario

The following is a sample scenario of the ACAS process:

An importer plans to import sneakers into the United States from Spain. Prior to the departure of the airplane from Spain to the United States, the filer submits the ACAS information as early as practicable, but no later than prior to loading of the cargo onto the aircraft. The filer has two options regarding their submission of the additional data elements: it can either submit all eighteen advance electronic manifest data elements in accordance with the ACAS timeline, or it can submit the ACAS data in the ACAS timeline, and all eighteen data elements in accordance with the 19 CFR 122.48a timeline.

CBP then performs a risk assessment regarding the carrier's ACAS filing. If the filing information is accurate, CBP provides an Assessment Complete message, which indicates that no risk has been identified, or that risks that were identified were satisfactorily mitigated. The captain of the aircraft then makes the determination that the items can be loaded on to the aircraft.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CBP operates the ACAS program pursuant to the following authorities: 19 CFR § 122.48a; Section 343(a) of the Trade Act of 2002, as amended; and 19 CFR § 122.41, which requires that all aircraft coming into the United States from a foreign area must make entry, subject to specified exceptions. The general authority for Air Commercial regulations is 5 U.S.C. § 301; and 19 U.S.C. §§ 58b, 66, 1415, 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, 1644a.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CBP maintains the ACAS information in ATS in accordance with DHS/CBP-006 Automated Targeting System.[23] The ATS SORN covers CBP's comparison of traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting rules and assessments to identify individuals and cargo that require additional scrutiny.

In addition, CBP is in the initial stages of drafting a new system of records notice specific to Cargo Security Records, which will cover ACAS and all records that CBP maintains for cargo security purposes

[23] 77 FR 30297 (May 22, 2012).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The ACAS Pilot was granted an Authority to Operate (ATO) on July 26, 2018, with an expiration date of January 25, 2020. The FIPS 199 determination for this system is moderate for confidentiality, integrity, and availability.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CBP retains ACAS data in accordance with the general ATS retention period of fifteen years, after which time it will be deleted. If information in ATS is linked to law enforcement lookout records or CBP matches to enforcement activities, investigations, or cases (i.e., specific and credible threats, flights, individuals, and routes of concern, or other defined sets of circumstances), that information will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related. CBP is developing a formal retention schedule for ATS and ACAS data for submission to NARA.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Yes. CBP's collection of ACAS information is covered under 1651-0001 Cargo Manifest/Declaration, Stow Plan, Container Status Messages and Importer Security Filing.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The following data elements are mandated under the ACAS program,[24] pursuant to 19 CFR 122.48b(d):

> (1) *Shipper name and address*. The name and address of the foreign vendor, supplier, manufacturer, or other similar party is acceptable. The address of the foreign vendor, etc., must be a foreign address. The identity of a carrier, freight forwarder, or consolidator is not acceptable.
>
> (2) *Consignee name and address*. This is the name and address of the party to whom the

[24] These data elements are defined in 19 CFR 122.48a(d)(1) for non-consolidated shipments and in 19 CFR 122.48a(d)(2) for consolidated shipments.

cargo will be delivered regardless of the location of the party; this party need not be located at the arrival or destination port.

(3) *Cargo description*. A precise cargo description or the 6-digit Harmonized Tariff Schedule (HTS) number must be provided. Generic descriptions, specifically those such as "FAK" ("freight of all kinds"), "general cargo," and "STC" ("said to contain") are not acceptable.

(4) *Total quantity* based on the smallest external packing unit. For example, 2 pallets containing 50 pieces each would be considered 100, not 2.

(5) *Total weight of cargo.* This may be expressed in either pounds or kilograms.

(6) *Air waybill number*. The air waybill number must be the same in the ACAS filing and the 19 CFR 122.48a filing. For non-consolidated shipments, the air waybill number is the International Air Transport Association (IATA) standard 11-digit number, as provided in 19 CFR 122.48a(d)(1)(i). For consolidated shipments, the air waybill number is the HAWB number. As provided in 19 CFR 122.48a(d)(2)(i), the HAWB number may be up to 12 alphanumeric characters (each alphanumeric character that is indicated on the HAWB must be included in the electronic transmission; alpha characters may not be eliminated).

These data elements are a subset of the eighteen advance electronic manifest data elements which are enumerated in 19 C.F.R. § 122.48a. If the shipper and/or consignee are individuals representing themselves (as a business), then names, addresses, and other contact information is submitted along with tax identification numbers (TIN) or Social Security numbers (SSN) as part of the larger air-cargo programs, but these data elements are not collected specifically for this advance submission.

2.2 What are the sources of the information and how is the information collected for the project?

The ACAS data is received from the ACAS filers that file their information prior to the departure of cargo to the United States. Information is not received from commercial sources or from publicly available data.

2.3 Discuss how accuracy of the data is ensured.

CBP collects information directly from the ACAS filers. Filing the ACAS data comes with certain responsibilities. Failure to fulfill these responsibilities could result in CBP issuing liquidated damages and/or assessing penalties. The inbound air carrier and/or the other eligible ACAS filer are responsible for providing accurate data to CBP in the ACAS filing and updating that data if necessary, transmitting the data in a timely manner to CBP, resolving ACAS referrals

prior to departure of the aircraft, and responding to a DNL instruction in an expedited manner. CBP needs accurate and timely data to perform effective risk assessments. To ensure this, the inbound air carrier and/or other eligible ACAS filer is liable for the timeliness and accuracy of the data that they transmit.

2.4 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: CBP may receive inaccurate ACAS data filling information.

Mitigation: This risk is partially mitigated. CBP mitigates this risk by collecting information directly from the ACAS filers. In addition, ACAS referrals may be issued for cargo determined to have insufficient or inaccurate data. If a filer does not fulfill these responsibilities, CBP is authorized to issue penalties.

Privacy Risk: There is a risk CBP is collecting more data than is necessary under ACAS.

Mitigation: This risk is mitigated. CBP requires only six individual data elements to be submitted in advance. All of these data elements were previously required, with the only change being the timeline requirement for submission. CBP explains in the instructions to ACAS filers which elements are mandatory.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Receiving information early from ACAS through ATS allows CBP to conduct targeting and risk assessment in ATS of shipments prior to the loading of aircraft destined for the United States. This process increases security by employing a risk-based approach to improve air-cargo security through targeted screening. Based on this risk assessment, CBP selects shipments that require additional information or screening, and receiving the information earlier allows CBP to halt shipments that may pose security risks before they are loaded on U.S.-bound aircraft.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

ACAS data is stored in ATS, which builds a risk-based assessment for cargo and conveyances based on criteria and rules developed by CBP. ATS cargo relies on rules-based targeting to build a score for the cargo or conveyance to subsequently identify cargo and/or conveyances of interest.

3.3 Are there other components with assigned roles and responsibilities within the system?

TSA also has responsibilities for securing inbound air cargo bound for the United States and may access ACAS data in ATS. CBP and TSA employ a layered security approach to secure inbound air cargo, including using various risk assessment methods to identify high-risk cargo and to mitigate any risks identified.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is risk that a traveler, conveyance, or cargo may be referred to secondary inspection even though that traveler, conveyance, or cargo does not present any risk of harm to the United States and has not committed or been associated with any violation of U.S. law based on the assignment of a risk score.

Mitigation: This risk is mitigated. CBP uses rules-based targeting to develop risk-based scoring for *cargo and conveyances only*. CBP relies on rules-based targeting to build a score for the cargo or conveyance to subsequently identify cargo and/or conveyances of interest. Persons associated with cargo shipments are screened against TECS lookouts and prior law enforcement actions to permit any identified violations to be considered as part of the overall score. Travelers identified by risk-based targeting scenarios are not assigned scores.

Privacy Risk: The privacy risks associated with the use of ACAS information maintained in ATS include the misuse of data by users.

Mitigation: Access to ACAS data in ATS is role-based, and ATS user roles are highly restricted and audited. Access is restricted in the form of Mandatory Access Control, which is based on a demonstrated "need to know." Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP Officers with access to ATS are required to complete security and data privacy training on an annual basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBP provides notice to the public of the ACAS program requirements through the regulation and its associated documentation (Federal Register notice, interim, and final rules). The CBP website provides information about ACAS, including fact sheets and frequently asked

questions, an implementation guide, and a link to the ACAS regulation.[25] In addition, this PIA provides general notice of CBP's collection and use of ACAS data.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

There is no opportunity to opt out of this collection. United States law requires persons seeking to import goods and merchandise in the United States to provide certain information to allow CBP to determine whether the goods/merchandise may enter the United States.

4.3 Privacy Impact Analysis: Related to Notice

There is no risk to notice regarding the ACAS program. CBP has published extensive Federal Register notices and rulemakings, as well as a dedicated page on its public-facing website about the ACAS program. CBP is publishing this PIA to assess the privacy risks and mitigations associated ACAS data and ensure transparency of its operations. The ATS PIA provides additional notice related to the system's capabilities.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

CBP retains ACAS information in ATS for 15 years. If ACAS information 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), it will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that CBP will retain information beyond the existing retention period.

Mitigation: This risk is partially mitigated. CBP will adhere to the designated 15-year retention schedule for ACAS. The data is retained in ATS consistent with CBP's practice for retaining information used to screen and target cargo and conveyances for border security and counterterrorism purposes. In the event that ACAS information becomes associated with a law enforcement investigation, CBP will maintain that information for as long as is required for the life of the investigation, which may exceed 15 years.

[25] https://www.cbp.gov/border-security/ports-entry/cargo-security/acas.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it will be used.

ACAS information, as warranted by specific request or Memorandum of Understanding, will be shared on a "need to know" basis, particularly with appropriate federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, when DHS believes the information would assist enforcement of civil or criminal laws. For targeting purposes, there are occasions in which certain data elements are shared outside of DHS to garner assistance in vetting and information gathering. At times, this is done in collaboration with intelligence community partners who may have additional information not available to CBP.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing outlined above is consistent with the purpose of CBP's original collection of the information, which supports CBP's enforcement of numerous federal laws at the border, and consistent with the broader CBP mission of safeguarding the nation while facilitating legitimate trade and travel.

6.3 Does the project place limitations on re-dissemination?

When sharing information pursuant to a memorandum of agreement, CBP requires that the recipient first request permission from CBP prior to sharing any information with a third party. External users of ATS with access to ACAS information must meet the terms and conditions of the arrangements permitting their access to ATS in order to obtain and maintain access. Generally, CBP requires that the external users employ the same or similar security and safeguarding precautions as employed by CBP and only use the data for legitimate purposes. For CBP, ATS has role-based security. Users from other government organizations must use the ATS interface to access the system where access is limited via a user profile/role. ATS user roles are highly restricted and audited. Application access is restricted in the form of role-based access, which is based on a demonstrated need to know. Users may not re-disseminate information without prior express written consent by CBP.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Information shared outside of the Department is tracked through the use of the DHS-191, Accounting of Disclosure Form, or a Memorandum of Understanding (MOU). All ATS users prepare a DHS-191 form each time they share PII from ATS outside of DHS. CBP and DHS share information from ATS pursuant to the terms of an arrangement for access to one or more of the modules of ATS, or in accordance with the language of a letter of authorization, which facilitates the sharing of a limited number of records from ATS in response to a request for assistance from another law enforcement agency.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that CBP will share ACAS data under inappropriate circumstances, or with individuals without a demonstrated need to know.

Mitigation: Risks related to sharing of information outside DHS, including any potential risk of further dissemination of information by the external agency to a third agency, are mitigated through arrangements governing access to ACAS information in ATS by external parties and sharing of ATS information with external parties. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being accessed or shared and the legal basis upon which they receive it. The arrangements generally require the external party accessing or receiving information to employ measures relating to security, privacy, and safeguarding of information that are equivalent or comparable to measures employed by DHS. As a general matter, the arrangements also stipulate that any further dissemination of ATS information by the receiving party to a third party is subject to prior authorization by CBP. Lastly, CBP emphasizes that within each arrangement, each external user is provided with training designed to ensure that data accessed through ATS is safeguarded and secured in an appropriate manner and that dissemination restrictions are observed, consistent with applicable laws and policies.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to ACAS information may file a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection
Freedom of Information Act Division
1300 Pennsylvania Avenue NW, Room 3.3D

Washington, D.C. 20229
Fax Number: (202) 325-1476

All Privacy Act and FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Requests for information are evaluated by CBP to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

Because ATS data related to risk assessments of ACAS data is by its very nature law enforcement sensitive, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemption in place. To the extent that a record is exempted in a source system, the exemption will continue to apply.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national 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 in accordance with procedures and points of contact published in the applicable SORN.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Inquiries and efforts to request correction of CBP records may be directed to:

U.S. Customs and Border Protection
CBP Info Center
Office of Public Affairs
1300 Pennsylvania Avenue NW
Washington, D.C. 20229

Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

7.3 How does the project notify individuals about the procedures for correcting their information?

CBP provides a variety of materials to commercial transport companies advising them how to submit information to CBP through ACAS. More generally, this PIA and the applicable SORNs provide general notice regarding the procedures for correcting ACAS information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: ACAS filers may be adversely impacted by the CBP cargo screening process based on a few select data elements.

Mitigation: CBP has designed the ACAS filing process to ensure that the importation and entry process is secure and seamless for the filer. In the majority of cases in which CBP issues a referral, the only requirement on the filer is to provide additional information, or for the cargo to undergo additional screening, much of which is non-intrusive and requires no effort on the part of the filer. Filers who do believe that they have been adversely impacted may seek redress as described in this PIA and the applicable SORNs. CBP seeks to permit all persons to be able to obtain copies of the ACAS data that the relevant importer submitted to CBP pursuant to regulatory requirements. As noted above in paragraph 7.3, individuals may also seek access to such information submitted to CBP pursuant to the FOIA, and as a matter of CBP policy, redress may also be requested.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

ACAS information is only available to users via ATS, which has role-based access. All user groups have access to the system as defined by their specific profile. Access is restricted based on roles and a demonstrated need to know.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Initial ATS access is not activated for any user without completion of the CBP Security and Privacy Awareness course. The course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official information and PII. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and ATS users are required to take the course annually.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Each user group's access to information in ATS is defined by the specific profile created for that group. Group profiles are intended to limit access by reference to the common rights and mission responsibilities of users within the group. Access by Users, Managers, System Administrators, Developers, and others to the ATS data is defined in the same manner and employs

profiles to tailor access to mission or operational functions. User access to data is based on a demonstrated need-to-know by a user, and access is only granted with supervisory and upon completion of the required security checks.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any access agreements that are put into place for ACAS program data will be drafted by the business owners with input from the program managers. Each agreement will define the nature of access to ATS for ACAS, including specific modules and scope of information subject to the sharing agreement. All information arrangements are reviewed by the CBP Privacy Officer and the CBP Office of Chief Counsel in accordance with existing CBP and DHS policy.

Responsible Officials

Dennis McKenzie
Deputy Executive Director
Manifest and Conveyance Security Division
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security