Privacy Impact Assessment
for the

Automated Commercial System (ACS)/ Automated Commercial Environment (ACE)- Importer Security Filing Data

December 2, 2008

Contact Point
Richard DiNucci
Director, Border Targeting and Analysis
Office of Field Operations
Customs and Border Protection
(202) 344-2513

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

Abstract

U.S. Customs and Border Protection (CBP) is expanding and revising the collection of data from carriers and importers to the Automated Commercial System (ACS) in an effort to prevent terrorist weapons from being transported to the United States. Using ACS, CBP collects cargo, carrier, importer, and other data to achieve improved high-risk cargo targeting as required by Section 203 of the Security and Accountability for Every Port Act of 2006 (Pub. L. 109-347, 120 Stat. 1884 (SAFE Port Act)). This PIA is being conducted to explore the use of personally identifiable information contained in the Importer Security Filing submitted by the importer to CBP.

Overview

Overview of the Automated Commercial System

The Automated Commercial System (ACS) is the comprehensive system used by U.S. Customs and Border Protection to track, control, and process all commercial goods imported into the United States. . Through the use of Electronic Data Interchange (EDI), ACS facilitates merchandise processing, significantly cuts costs, and reduces paperwork requirements for both Customs and the importing community. Within ACS are several methods for EDI, two of which are the Automated Broker Interface (ABI) and the Automated Manifest System (AMS). Under the "10+2" program, importers submit the Importer Security filing using ABI or Vessel AMS, systems under ACS, to CBP. The data is immediately sent to the Automated Targeting System (ATS) for targeting purposes, and then returned to ACS for retention.

Automated Broker Interface (ABI)

The Automated Broker Interface (ABI) is an integral part of ACS that permits qualified participants to file import data electronically with Customs. ABI is a voluntary program available to brokers, importers, carriers, port authorities, and independent service centers. Currently, over 96% of all required entries are filed through ABI.

ABI expedites the release of merchandise to the trade community because it allows CBP to begin processing the import in advance of the merchandise arriving at the port of entry. Entry summaries are electronically transmitted, validated, confirmed, corrected, and paid. Administrative messages keep participants informed of all current information and issues.

Participants can query quota status, visa requirements, manufacturer information, and entry/entry summary processing status. ABI allows filers to pay multiple entries with one payment transaction through statement processing. ABI filers can also pay Customs duties, fees, and taxes electronically through the Automated Clearinghouse (ACH).

Automated Manifest System

The Automated Manifest System (AMS) handles manifest information provided by the carrier (rather than the importer) and notifies the carrier when the merchandise can be transported from the port of entry. AMS interfaces directly with the Cargo Selectivity and In-Bond systems of ACS, and indirectly with ABI. This linkage allows faster identification and release of low risk shipments. AMS speeds the flow of cargo and entry processing that provides participants with electronic authorization of cargo prior to arrival. AMS facilitates the inter-modal movement and delivery of cargo by rail and trucks through the In-bond

system. Sea, air and rail carriers, port authorities, service bureaus, freight forwarders, rail carriers, and container freight stations can participate in AMS. AMS reduces reliance on paper documents and speeds the processing of manifest and waybill data. As a result, cargo remains on the dock for less time, participants realize faster tracking, and Customs provides better service to the importing community.

Vessel AMS allows participants to transmit manifest data electronically prior to vessel arrival. Customs can then determine in advance whether the merchandise merits examination or immediate release. Upon receiving notification from Customs, the carrier can make decisions on staging cargo and the importer can arrange for examination, release, and distribution of the merchandise. All of this can be accomplished before the merchandise arrives. Vessel AMS allows communication between AMS participants and other government agencies, container freight stations, and non-vessel operating common carriers.

Overview of "10+2":

To help prevent terrorist weapons from being transported to the United States, vessel carriers bringing cargo to the United States are required to transmit certain information to Customs and Border Protection (CBP) about the cargo they are transporting prior to lading that cargo at foreign ports of entry. CBP is issuing an interim final rule that requires both importers and carriers to submit additional information pertaining to cargo to CBP before the cargo is brought into the United States by vessel. This information must be submitted to CBP by way of a CBP-approved electronic data interchange system. The required information is necessary to improve CBP's ability to identify high-risk shipments so as to prevent smuggling and ensure cargo safety and security, as required 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.

The proposed rule was known to the trade as both the "Importer Security Filing proposal" and the "10 + 2 proposal." The name "10 + 2" is shorthand for the number of advance data elements CBP was proposing to collect. Carriers would be generally required to submit two additional data elements - a vessel stow plan and container status messages regarding certain events relating to containers loaded on vessels destined to the United States - to the elements they are already required to electronically transmit in advance (the "2" of "10+2"); and importers, as defined in the proposed regulations, would be required to submit ten data elements - an Importer Security Filing containing ten data elements (the "10" of "10+2").

Carriers are currently required to submit advance cargo information for vessels, including a vessel's Cargo Declaration, to CBP via the Vessel Automated Manifest System (AMS). Carriers are currently not required to submit Vessel Stow Plans (VSPs) or Container Status Messages (CSMs) to CBP. In addition, importers of record are generally required to file entry information, including CBP Form 3461, with CBP within fifteen calendar days after or before the date of arrival of a shipment at a United States port of entry and entry summary information, including CBP Form 7501, within ten working days after or before the entry of the merchandise. Entry and entry summary information is submitted to CBP via the Automated Broker Interface (ABI) or via paper forms. Importers are not currently required to submit advance cargo information to CBP.

The interim final rule being issued requires carriers to submit VSPs and CSMs and importers to submit Importer Security Filings (ISFs) to CBP. This data is known collectively as "10+2" data. The carrier submissions, the VSPs and CSMs, do not contain any personally identifiable information, so they will not be the focus of this PIA. This PIA will focus on the importer submission, the ISF, which may contain personally identifiable information.

Importer Security Filings:

This final rule requires ISF Importers, as defined in these regulations, or their agents, to transmit an ISF to CBP, for cargo other than foreign cargo remaining on board (FROB), no later than 24 hours before cargo is laden aboard a vessel destined to the United States. Because FROB is frequently laden based on a last-minute decision by the carrier, the ISF for FROB is required any time prior to lading. An ISF is required for each shipment, at the lowest bill of lading level (i.e., at the house bill of lading level, if applicable). The party required to submit the ISF is the party causing the goods to enter the limits of a port in the United States. This party is the carrier for FROB and the party filing for the immediate exportation (IE), transportation and exportation (T&E), or foreign trade zone (FTZ) documentation for those types of shipments. The ISF Importer, as a business decision, may designate an authorized agent to file the ISF on the ISF Importer's behalf. A party can act as an authorized agent for purposes of filing the ISF if that party obtains access to ABI or AMS.

ISF Importers, or their agents, must transmit the ISF via a CBP-approved electronic data interchange system. The current approved electronic data interchange systems for the ISF are ABI and vessel AMS. The party who filed the ISF must update the ISF if, after the filing and before the goods arrive within the limits of a port in the United States, there are changes to the information filed or more accurate information becomes available.

ISF Importers, or their agents, must submit ten elements to CBP for shipments consisting of goods intended to be entered into the United States and goods intended to be delivered to an FTZ (see 1.1 below). ISF Importers, or their agents, must submit five elements to CBP for shipments consisting entirely of FROB and shipments consisting entirely of goods intended to be "transported" as IE or T&E in-bond shipments (see 1.1 below).

Two of the ISF elements are identical to elements submitted for application to admit goods to an FTZ (CBP Form 214). These elements are the country of origin and commodity Harmonized Tariff System of the United States (HTSUS) number when provided at the ten-digit level. The filer may submit the ISF and CBP Form 214 in the same electronic transmission to CBP and may submit the country of origin and commodity HTSUS number once to be used for both ISF and FTZ admission purposes. If the party submitting the ISF chooses to have this element used for FTZ admission purposes, the HTSUS number must be provided at the ten-digit level.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

For shipments other than those consisting entirely of FROB and goods intended to be "transported" in-bond as an Immediate Exportation (IE) or Transportation and Exportation (T&E), the ISF

must consist of ten elements, unless an element is specifically exempted. The manufacturer (or supplier), country of origin, and commodity Harmonized Tariff Schedule of the United States (HTSUS) number must be linked to one another at the line item level. The ten elements are as follows:

(1) Name and Address of Manufacturer (or supplier);
(2) Seller (full name and address or a widely accepted industry number such as a DUNS number);
(3) Buyer (full name and address or a widely accepted industry number such as a DUNS number);
(4) Ship to party (full name or company name and address);
(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.

For shipments consisting entirely of FROB and shipments consisting entirely of goods intended to be "transported" in-bond as an IE or T&E, the Importer Security Filing must consist of five elements, unless an element is specifically exempted. The five elements are as follows:

(1) Booking party (*i.e.*, name and address);
(2) Foreign port of unlading;
(3) Place of delivery;
(4) Ship to party (full name or organization and address); and
(5) Commodity HTSUS number.

In addition to above information collected on the ISF, CBP collects information related to the importer, which may include the importer of record number, which can be the social security number or employee identification number (EIN), and the bond agent and his social security number or EIN. This information is part of the entry transaction and is maintained separately from the ISF.

As a result of the screening and targeting in ATS and consistent with the existing ATS SORN, links or pointers to specific transactions and those aspects of the transaction which matched rule sets in ATS and contributed to the risk assessment and score will be inserted into the data and sent back to ACS. The links or pointers, rule sets, and scores will be retained in ATS.

1.2 What are the sources of the information in the system?

The data elements are collected from the ISFs completed by the importers or their authorized agents. Importers or their agents, submit the data elements via vessel AMS or ABI.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is being collected to provide advanced notice of importer cargo for targeting and safety purposes. The data will be temporarily stored in ACS, forwarded to ATS for targeting purposes, then sent back to ACS for retention. This temporary storage is necessary, because ACS encompasses the Vessel

AMS and ABI, which are the authorized channels for submitting cargo information. Further, temporary storage in ACS is needed for message control (confirming the receipt and routing of incoming data). Once the data has been processed by ATS, the data is returned to ACS with links from the results of ATS targeting and screening. Once returned, the data is stored in ACS according to the normal retention schedule for ACS data.

1.4 How is the information collected?

Importers must enroll in the ABI or Vessel AMS program to set up a profile. Once CBP has created a profile for the importer, the importer uses authorized software to submit data electronically via the secure Vessel AMS and ABI systems under ACS.

1.5 How will the information be checked for accuracy?

Importers are responsible for filing an accurate ISF. The accuracy and timeliness of Importer Security Filings is secured by an importer's bond and CBP may issue fines for inaccurate information. The system permits importers, or their agents, to file a new ISF if they find they have filed inaccurate information.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

This collection is required 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.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

CBP recognizes that the information provided is sensitive to the importer, individuals, and other parties involved. However, these data elements are needed to achieve the statutorily required purposes of improved high-risk cargo targeting. In order to protect the personally identifiable information submitted by the importer, CBP is using already existing, proven systems for transferring the information. CBP already deploys extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of CBP employees. CBP's physical security measures include maintaining the information systems and access terminals in controlled space protected by armed individuals. Access to information is restricted by role, responsibility, and geographic location of the employee accessing the information.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information provided will temporarily reside in ACS before being forwarded to ATS. During the initial storage in ACS, data may be accessed by CBP to confirm receipt to the party that transmitted it and to rout the information to ATS. Once the data is transmitted to ATS, it is processed for targeting and screening purposes. Once the data has been processed by ATS, ATS will insert links to specific data elements from the results of the targeting and screening, and the data will be returned to ACS for retention according to the retention schedule (see 3.2 below).

Where indicated by the importer, the ISF may be submitted both for 10+2 purposes and as a 7501 Entry Summary. In these cases, the data will be copied into ACS as both and treated according to the separate uses.

2.2 What types of tools are used to analyze data and what type of data may be produced?

ACS will not analyze the ISF data. Rather, ACS will send the ISF data to ATS, which will use the information for targeting and screening purposes. Separately, ACS employs its Cargo Selectivity Module to screen transactions as a means of determining which cargo requires further inspection or examination.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

As with any collection of personally identifiable information, there is a risk of misuse of the information. To mitigate this risk, access to data in ACS is controlled through passwords and restrictive rules. Users are limited to the roles that define authorized use of the system. Procedural and physical safeguards are utilized such as accountability and receipt records. Management oversight is in place to ensure appropriate assignment of roles and access to information.

In order to become an authorized user, an officer must have successfully completed privacy training and hold a full field background investigation. Finally, an officer must not only complete the above, but must have a "need-to-know" for the information.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

All the data elements listed above are retained. (See 1.1).

3.2 How long is information retained?

Data is sent immediately to ATS upon receipt and confirmation in ACS. Once ATS has processed the data for targeting and screening purposes, it will send back the ISF to ACS for retention consistent with information collected for a border security or counter-terrorism purpose, which is 15 years.

Where the importer has indicated that the ISF should also be considered a 7501 Entry Summary, it will be retained in ACS according to the normal retention schedule for 7501 Entry Summaries.

Information related to entry of merchandise will maintained for six years because this is the statute of limitations for pursuing penalties or related legal action.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

No. A review of the record retention and disposition schedule for ACS is being planned with NARA.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

CBP retains the data for a period of 15 years; the data is not archived or kept in any form after the listed retention period. The data is retained in ACS consistent with CBP's practice for retaining information used to screen and target persons and business entities for border security and counter-terrorism purposes. Access to the ISF is limited to uses consistent with the purpose for retention and is restricted to those officers and employees with a mission related responsibility concerning the counter-terrorism or law enforcement purpose for which the information was collected.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

CBP may share the VSP, CSM, and ISF data with other components within DHS where there is a need to know in accordance with their responsibilities, including collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. These DHS components may include ICE, TSA, and I& A.

4.2 How is the information transmitted or disclosed?

The information may be transmitted either electronically or as printed materials to authorized personnel. CBP's internal data sharing is required to comply with statutory requirements for national security and law enforcement systems. Access terminals, mainframe processors, and databases are all maintained in DHS controlled space protected by armed guards. Hard copies of information are protected by sealed envelope and shared via official intra-agency courier. All information is kept secure, accurate, and controlled. Authorized personnel must possess a mission or job related need and intended use before access may be granted.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

In order to mitigate the privacy risks of personally identifiable information being inappropriately used, the information is shared only with DHS personnel who have a need to know the information as part of the performance of their official employment duties. Internal DHS access to ACS data is controlled by CBP through the use of strict access controls for the users, passwords, background checks for individuals accessing the data, as well as system audits that track and report on access to the data. Additionally, any individual with access has gone through privacy training.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

DHS counter-terrorism, law enforcement and public security communities will be provided with information about suspected or known violators of the law and other persons of concern uncovered via ISF data in a timely manner. The 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, where DHS believes the information would assist enforcement of civil or criminal laws.

Presently, this external sharing includes every counter-terrorism and law enforcement agency in the Federal government, as well as those Federal agencies mandated to ensure compliance with laws or regulations pertaining to entry into or exit from the U.S., each of the Fifty States, the District of Columbia, U.S. insular possessions and territories, and a majority of foreign nations with which the U.S. maintains diplomatic relations.

All 10+2 information collected is subject to being shared for reasons of general law enforcement, counter-terrorism purposes, border, aviation, sea, rail, and public security.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Personally identifiable information (PII) is shared outside the department according to the provisions of the Privacy Act (5 U.S.C. 552a) and the routine uses listed in the accompanying ACS SORN for the purposes listed above. See 5.1.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information may be transmitted either electronically or as printed materials to authorized personnel. CBP's external data sharing of the data submitted to ACS is required to comply with statutory requirements for national security and law enforcement systems. All information is kept secure, accurate and controlled. Additionally, Memoranda of Understanding and other written arrangements, defining roles

and responsibilities, have been executed between CBP and each agency that regularly accesses ACS. Lastly, information that is shared with other agencies, Federal, state, local, tribal, or foreign, outside of the context of any MOU or other prior written arrangement requires a written request by the agency specifically identifying the type of information sought and the purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the Chief, Privacy Act Policy and Procedures Branch, Regulations & Rulings, Office of International Trade, CBP, insofar as the request and use are consistent with the Privacy Act, the published routine uses for ACS, and the receiving agency agrees to be restricted from further unauthorized sharing of the information. All three requirements—use consistent with purpose for collection, sharing consistent with a statutory or published routine use, and acceptance of the restriction barring unauthorized dissemination outside the receiving agency—and the legal responsibility clause for wrongful dissemination contained in the Paperwork Reduction Act (44 U.S.C. section 3510) are stated as conditions pertaining to the receiving agencies acceptance and use of the shared information. These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

Recipients of 10+2 data are required by the terms of their sharing arrangement (including an MOU) to employ the same or similar precautions as CBP in the safeguarding of information that is shared with them. CBP requires all external users of ACS (that is, external to CBP) to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in ACS. This training is available online, once a user has met the background requirements for access to ACS. The training module must be completed prior to a user accessing other functionality within the ACS environment.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

When sharing information with third parties, the same specifications related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the interface request and the implications on privacy related concerns are two factors that are included in both the initial and ongoing authorization, the written arrangement (MOU) and Interconnection Security Agreement that is negotiated between CBP and the external agency that seeks access to CBP data. The written arrangement specifies the general terms and conditions that govern the use of the functionality or data, including limitations on use. The Interconnection Security Agreement ("ISA") specifies the data elements, format, and interface type to include the operational considerations of the interface. The written arrangements and ISAs are periodically reviewed and outside entity conformance to use, security, and privacy considerations is verified before Certificates to Operate are issued or renewed.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

CBP will collect this information directly from the relevant carriers and importers by regulation and will provide notice through publication of 10+2 "Importer Security Filing and Additional Carrier Requirements" Interim Final Rule, as well as this privacy impact assessment and updated ACS SORN. Carriers and importers are already notified and required to provide similar information to ACS using the same channels. CBP will also work with the trade on ongoing issues and will keep updating and posting new FAQs to the CBP website, while conducting additional outreach to the trade and various foreign government entities.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

No. CBP may take enforcement action against a carrier that fails to comply with the requirement to submit stow plans in a timely or accurate manner. CBP enforcement actions may include, but are not limited to, claims for liquidated damages pursuant to 19 CFR 113.64(f). However, CBP has set a compliance date of one year from the effective date of this final rule.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. Individuals do not have the right to consent to particular uses of the information. Carriers and importers must provide the required information in a timely manner and may not exercise control over the data thereafter.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is a risk that importers may not know to provide the information. However, CBP is taking the steps enumerated above to notify the importing community about these requirements. See 6.1.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

DHS allows persons, including foreign nationals, to seek access under the Privacy Act to certain information maintained in ACS. Requests for access to personally identifiable information contained in ACS, that was provided by the carrier or importer regarding 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). However, records and information maintained in ACS pertaining to the results of targeting or other derogatory information cannot be accessed.

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.

In addition, the Freedom of Information Act (FOIA) (5 U.S.C. 552) provides a means of access to information, including ACS data, for all persons, irrespective of the individual's status under the Privacy Act. With respect to data for which ACS is the actual source system, the ACS SORN is published in the Federal Register. FOIA requests for access to information for which ACS is the source system may be directed to CBP in the manner prescribed by regulations at Title 19, Code of Federal Regulations, Part 103.

7.2 What are the procedures for correcting inaccurate or erroneous information?

CBP has an Executive Communications Branch in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems (including ACS). If an individual believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to the Customer Service Center, at the following address: Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511). Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. Individuals may provide additional information to CBP to ensure that the information maintained by CBP is accurate and complete. The Customer Service Center will respond in writing to each inquiry.

Individuals and foreign nationals may also seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). Persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through TRIP. TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports and train stations or at U.S. land borders. Through TRIP, a traveler can request

correction of erroneous data stored in ACS and other data stored in other DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA- 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

7.3 How are individuals notified of the procedures for correcting their information?

With respect to information about an individual, collected from an importer and submitted to CBP, ACS is not exempt from the amendment provisions of the Privacy Act. In the course of any access or amendment process by that person, or his or her agent, to whom the biographical or other data associated with this SORN pertains, the Customer Service Center will explain the procedures for amendment. However, law enforcement or investigatory records or their links to information maintained in ACS pertaining to the individual are exempt from the access and amendment provisions of the Privacy Act. Requests for redress should be directed to CBP's Customer Service Center (see section 7.2. above).

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

As set forth in the ACS SORN published in the Federal Register, CBP provides access and amendment in ACS to the data obtained from the importer about a person or obtained directly from the individual at the time of physical processing of an entry record at the border. In doing so, CBP seeks to permit all persons to be able to obtain copies of the ACS data that the relevant importer submitted to CBP pursuant to regulatory requirements. As noted above in paragraph 7.1, individuals may also seek access to such information submitted to ACS pursuant to the FOIA, and as a matter of CBP policy, redress may also be requested in the manner described above in paragraph 7.2.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Importers, their agents, or other individuals whose personal information is collected by ACS will not have access to their information through Vessel AMS or ABI after the ISF has been submitted. Importers and their agents will not be able to view any data once it has been submitted. Importers, or their agents, will only be able to see the confirmation that the ISF is filed. After submission, applicants may update their ISFs by submitting an update.

Access to the system is granted and limited to a need to know basis. All parties with access to the system are required to have full background checks. The universe of persons with access includes CBP Officers, DHS employees, Federal counter-terrorism, law enforcement and public security officers, IT specialists, program managers, analysts, contractors, and supervisors of these persons.

8.2 Will Department contractors have access to the system?

Yes, subject to the same background, training, need-to-know, and confidentiality requirements as employees.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All users of the ACS system are required to complete and pass annual TECS Privacy Act Course (TPA) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the user's understanding of appropriate controls put in place to protect privacy as they are presented. A user must pass the test scenarios to retain access to ACS. This training is regularly updated.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

ACS received an approved Certification and Accreditation under the National Institute of Standards and Technology on March 23, 2006. This C&A is valid for a period of three years.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Every six months a user must request and his or her immediate supervisor must reauthorize access to ACS. Reauthorization is dependent upon a user continuing to be assigned to a mission role requiring ACS access and the absence of any derogatory information relating to past access.

ACS transactions are tracked and can be monitored. This allows for oversight and audit capabilities to ensure that the data are being handled consistent with all applicable laws and regulations regarding privacy and data integrity. ACS maintains audit trails or logs for the purpose of reviewing user activity. ACS actively prevents access to information for which a user lacks authorization as defined by the user's role in the system, location of duty station, and/or job position. Multiple attempts to access information without proper authorization will cause ACS to suspend access automatically. Misuse of ACS data can subject a user to discipline in accordance with the CBP Code of Conduct, which can include being removed from an officer's position.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks identified with respect to access and security were in appropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, the CBP Code of Conduct and Disciplinary system, and the practice of least privileged access.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

ACS is a legacy trade and commercial compliance system used to process all imported merchandise into the United States. ACS allows for the tracking of cargo movement and the assignment of classification and duty assessments with regard to imports.

9.2 What stage of development is the system in and what project development lifecycle was used?

ACS is an operational system in current production. This PIA is provided to address an expansion of the types of information and individuals participating in international trade and related transactions, who are subject to its collection requirements. Integrity, privacy, and security were analyzed as part of the decisions made for ACS in accordance with CBP security and privacy policy from the inception of ACS, as demonstrated by the successful transition through the systems development lifecycle (SDLC), certification and accreditation, and investment management processes. Particular areas that were identified as needing to be addressed during the development included: use of accurate data, system access controls, and audit capabilities to ensure appropriate use of the system.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

ACS is a legacy system that has been updated to address the additional elements that are required to be submitted under the 10+2 interim final rule. No additional privacy risks were found during the analysis of this PIA.

Responsible Officials

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.

Richard DiNucci, Director, Border Targeting and Analysis, Office of Field Operations, U.S. Customs and Border Protection, (202) 344-2513

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security