Privacy Impact Assessment

for

Automated Commercial Environment (ACE)

e-Manifest: Trucks (ACE Release 4) and

International Trade Data System (ITDS)

July 14, 2006

Point of Contact:

Laurence Castelli

Office of Regulations and Rulings / Office of Information Technology

U.S. Customs and Border Protection

(202) 572-8712

Reviewing Official:

Maureen Cooney

Acting Chief Privacy Officer

U.S. Department of Homeland Security (DHS)

(571) 227-3813

Introduction

U.S. Customs and Border Protection (CBP) is engaged in a multi-year modernization effort to update its information systems. This modernization effort began in 2001 with the development of the Automated Commercial Environment (ACE) as a replacement for CBP's current Automated Commercial System (ACS), a twenty plus year old trade information database. The purposes of ACE are to streamline business processes, to facilitate growth in trade, to ensure cargo security, to provide means to combat terrorism through monitoring what materials and which persons enter and leave the country, and to foster participation in global commerce, while ensuring compliance with U.S. laws and regulations. Development of ACE will consist of many releases. Each release, while individually achieving critical business needs, will also set forth the foundation for the subsequent releases.

To build on existing infrastructure, ACE will use the International Trade Data System (ITDS) to share electronic international trade and transportation data with Participating Government Agencies (PGAs) of the Federal government. ITDS provides the Federal government with a secure, integrated, government-wide interface for disseminating and using this information. Through the ITDS interface, ACE will allow for a one-stop automated mechanism for enforcing hundreds of U.S. laws and international trade and transportation requirements in partnership with and on behalf of all interested federal agencies by sharing international trade and transportation data.

PGAs are any other Federal Agency that requires access to the information being collected by ACE and has signed a Memorandum of Understanding (MOU) regarding the appropriate use of the information. As an example, the first participating government agency, the Federal Motor Carrier Safety Administration (FMCSA), a division of the U.S. Department of Transportation (DOT) will receive carrier information on trucks crossing the borders submitted to ACE via carrier electronic Manifests (e-Manifests) and will, in turn, verify certain data elements contained in this information to improve truck safety and regulatory compliance.

This PIA is based on the functionality encompassed in ACE's Release 4, e-Manifest: Trucks. FMCSA is the only PGA receiving and processing data from CBP under ACE's Release 4, pilot test. FMCSA, in addition, will issue its own PIA, which will be posted on the DOT web-site and will cover the FMCSA information systems and processes not relevant to CBP's mission. As other agencies participate in ACE, through the ITDS interface, and become PGAs, they will prepare PIAs, as appropriate, and publish these PIAs to their web-sites. Similarly, CBP will update this PIA as PGAs are added that have an impact on privacy.

With this release, ACE Truck Carrier Account-holders will have access to operational data, receive status messages on ACE Accounts, have access to integrated Account data from multiple system sources, manage and disseminate information in an efficient and secure manner, and obtain release of their cargo, crew, conveyances, and equipment. In addition, ACE will also be receiving electronic transmissions of Postal Declarations filed in conjunction with mail importations from the U.S. Postal Service.

To test the ACE e-Manifest, CBP is conducting a pilot that allows participating Truck Carrier Accounts to transmit electronic manifest or e-Manifest data into ACE (including advance cargo information) as required by section 343 of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002 (*see*, Volume 68, Federal Register (FR), 68140, dated December 5, 2003). Carriers were solicited to participate in this pilot by a notice published on February 4, 2004 (69 FR 5360), and the test was announced in a notice published on September 13, 2004 (69 FR 55167). This Federal Register notice was clarified, subsequently, by a further notice published on March 21, 2005 (70 FR 13514).

Implementation of the test was announced in a Federal Register notice on May 31, 2005 (70 FR 30964), in which CBP announced the sequencing of the testing as occurring at the original port of implementation, Blaine, Washington, and then expanding through the first cluster of subsequent ports in Washington State. In this last notice, CBP also stated that future deployment of the test would occur at

Champlain, New York; Detroit, Michigan; Laredo, Texas; Otay Mesa, California; and Port Huron, Michigan. CBP will announce sites and dates for future deployment of this test, as they are determined. CBP will process additional Truck Carrier Account applications as CBP expands the universe of participation for this functionality. As ACE adds new functionality and further implements Release 4, this PIA will be updated or a new PIA will be issued to discuss the privacy impact of the new systems.

Section One: Data Scope and Purpose

1.1 What information is to be collected?

To collect information about individuals, companies, and government employees involved in commercial border transactions, ACE will employ both Portal Accounts, in which individuals sign in and enter their own information through an internet based secure data portal, and Electronic Data Interfaces (EDI), in which trade and carrier accounts directly transmit their data through system to system connections. The ACE system database is composed of the following information:

- Truck carrier accounts information,
- broker account information,
- importer account information,
- electronic truck manifests (e-Manifests),
- U.S. Postal information on importations,
- CBP employee information, and
- information pertaining to employees of PGAs,

Truck Carrier Account Information

Truck Carrier account information in the ACE system database will consist of Carrier name, Carrier address, Carrier identification (i.e., the truck carrier identification Standard Carrier Alpha Code (unique code assigned for each carrier by the National Motor Freight Traffic Association)), U.S. Department of Transportation (DOT) number, Taxpayer ID number, Dun and Bradstreet Number (DUNS), Organizational structure, Name of Insurer, Policy number, Date of Issuance, and Amount. As for personal information stored in the account, the carrier can enter names and addresses to create account users and points of contact, and may also choose to store details associated with driver, crew, and passengers for purposes of expediting the creation of manifests.

Broker Account Information

Broker account information in the ACE system database will consist of company name and address, importer number, filer code, Taxpayer ID number, Dun and Bradstreet Number (DUNS) (if applicable), and organizational structure. Additionally, personal information relating to each individual authorized to use the Broker's portal account access will also be stored in the account information, this will include: individual name and address, broker's license number (if applicable), and business relationship.

Importer Account Information

Importer account information in the ACE system database will consist of company name and address, importer number, filer code, Taxpayer ID number, Dun and Bradstreet Number (DUNS) (if applicable), and organizational structure. Additionally, personal information relating to each individual authorized to use the Importer's portal account access will also be stored in the account information. This will include the individual's name, address, and business relationships.

E-Manifest Information

E-Manifest information in the ACE system database will consist of specific details regarding the trip, conveyance, equipment, crew, and shipments related to a commercial land border crossing. This information is accessed in the processing of commercial conveyances, their crew, equipment, and shipments. A truck manifest is made up of four parts: the crew, conveyance, equipment, and shipments. This information is collected from the e-Manifest submitted by the carriers to CBP. Subsequently, the data elements pertinent to FMCSA will be verified by FMCSA's Query Central, a clearinghouse database, which will interface with other FMCSA systems. For more information on FMCSA's processes and systems, see FMCSA's separate Privacy Impact Assessment, available on DOT's web-site. The following personal information is collected:

Crew/Driver
1) Name of person on arriving conveyance who is in charge 2) name/s of all accompanying crew members 3) date of birth of each accompanying crew member and the driver 4) Commercial Driver's License (CDL)/driver's license number for the driver and any accompanying crew member 5) CDL/driver's license state/province of issuance for the driver and any accompanying crew member 6) CDL country of issuance for the driver and any accompanying crew member 7) travel document number for each accompanying crew member and the driver 8) travel document country of issuance for each accompanying crew member and the driver 9) travel document state/province of issuance for each accompanying crew member and the driver 10) travel document type for each accompanying crew member and the driver11) destination address for each accompanying crew member and the driver 12) gender of each accompanying crew member and the driver13) nationality/citizenship of each accompanying crew member the driver14) hazmat endorsement for each accompanying crew member and the driver 15) Free and Secure Trade (FAST) Driver Proximity Card number.

Please note that if an individual serving as an accompanying crew member or driver has a FAST (Free and Secure Trade) Driver Proximity Card, the carrier (account holder) submits the card number and no other personal information about the individual. CBP FAST system transmits all personal information to ACE. For more information about FAST, refer to Section IV, Data Access, of this document.

Passenger
1) Name 2) date of birth 3) travel document number 4) travel document country of issuance 5) travel document state/province of issuance 6) travel document type for each passenger 7) gender 8) nationality.

U.S. Postal Information on Importations
The U.S. Postal information on importation in the ACE system database will consist of name and address of sender and recipient, as well as phone information and payment information associated with the party responsible for paying the duty owed on the imported merchandise.

CBP and PGA Employee Information
CBP and PGA employee information in the ACE system database will consist of employee name and Social Security Number (SSN) to ensure secure login. The SSN is translated into a "hash" ID code. The SSN itself is not visible on the ACE screen and ACE users do not have access to this information.

1.2 Why is the information being collected? Is it relevant and necessary to the purpose for which the system is being designed?

The e-Manifest information is collected in ACE to assist in protecting the country's borders by monitoring and regulating incoming cargo, vehicles (conveyances) and people. In this release 4, the information is specifically collected to increase efficiency of moving trade across the borders, to share

relevant trade and transportation data with appropriate PGAs, to identify suspicious individuals or cargo, and to identify non-compliant conveyances entering the United States. ACE is being designed both to facilitate legitimate trade and assist CBP in enforcing compliance with the various laws that govern the movement and means of movement of trade and people across the borders of the United States.

1.3 What is the intended use of the information?

The information from trade accounts, carrier accounts, e-Manifests, and the U.S. Postal Service is used to assist CBP and PGAs in monitoring the passage of commodities, materials, crewmembers, and passengers across U.S. borders. The information is also used by both the owners of the various accounts and the submitters of the information, being collected, to view the status of their respective transactions with CBP and other PGAs and to maintain a historical record of recent transactions for trend analysis, internal auditing, and compliance activities. CBP and PGA employee information is used to create user hash IDs to allow qualified CBP and PGA users access to the ACE system.

1.4 What are the sources of the information in the system? Where and how are you acquiring the information?

Personal information about the carrier's driver and/or crew is submitted by the account holder to the ACE system when creating an account in ACE or when submitting a manifest on a transactional basis (each time the truck crosses the border). If a driver is a holder of the FAST Driver Proximity Card, the information will be transferred from FAST to ACE. Information about an individual may also come from the Treasury Enforcement Communications System (TECS)/Interagency Border Inspection System (IBIS) database if a match or possible match is found during a query. The information from TECS/IBIS would consist of a statement indicating additional information is stored in the TECS database.

1.5 How will the information be checked for accuracy?

Personal information will be checked for accuracy manually by a CBP Officer cross-referencing the data obtained through ACE and other CBP systems with the identification information provided by the driver and accompanying crew upon arrival at the border.

Within the ACE system, quality control toolsets are employed to validate and reconcile data obtained from multiple sources. These tools focus on the following data quality characteristics to achieve this reconciliation: accuracy, precision, completeness, consistency, reliability, timeliness, uniqueness, validity, and data synchronization. Implementation of data quality measures include the following:

- External automated tools to examine the database for inter- and intra-field consistency and referential integrity constraints
- Use of data quality capabilities embedded within the Extract Transform and Load tools
- Analysis of execution logs.

1.6 Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

The system records whether the individual was allowed to enter the country. The system knows how many times, when, and where a driver, crewmember, or passenger crosses the border. The flexible querying tool used by ACE can order reports on the information collected by ACE, but the reports cannot be used to change an individual's existing records. This information recorded by ACE is used by the CBP Officer to determine whether or not to allow an individual into the country, and what, if any, action should be taken with respect to the merchandise being imported or mailed to a U.S. destination, or a vehicle being operated by the driver.

1.7 Will the newly derived data be placed on the individual's record?

The fact that the individual was or was not allowed to enter into the country is recorded in the individual's record in ACE. An enforcement action (*i.e.*, seizure or penalty) resulting from the seizure of a mail importation or of any importation will identify the individuals associated with the transaction involving the seized merchandise. Specific information regarding the enforcement action will reside in a separate system with ACE containing only a pointer to the reference in the other system.

1.8 Can the system make new determinations about an individual that would not be possible without the new data?

The ACE system is not able to make any new determinations with this information; the system assists the CBP Officer in making the appropriate determination about whether to allow an individual, merchandise, or conveyance into the country. Similarly, the ACE system will improve PGAs ability to make determinations with respect to data pertaining to their respective authorities. For example, once a Memorandum of Understanding (MOU) is executed between FMCSA and CBP, the FMCSA will use information collected through the ACE system to screen and provide clearance for carriers, cargoes, conveyances, and drivers/crews prior to their arrival at the border and to assist with safety enforcement once the carrier has entered the United States.

1.9 How will the newly derived data be verified for relevance and accuracy?

Not applicable.

1.10 Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in detail in the Interface Control Documents, the Multi-Modal Manifest Data Elements Matrix, and the Logical Data Model. Separately, the data elements were also published in the Federal Register at 70 FR 13514 on March 21, 2005.

Section 2: Data Modifications/Redress

2.1 What opportunities do individuals have to decline providing information?

If a truck carrier has agreed to participate in the pilot, then all relevant, requested information must be provided. With regard to truck drivers employed by participating carriers, the program is mandatory. There are no opportunities for the individual to decline providing information once the participating carrier has agreed to participate in the pilot. However, if the company has agreed to participate in the pilot, CBP strongly recommends that the account holder inform the individual whose personal data is reported to ACE, with respect to this fact. This recommendation can be found in the CBP Privacy Policy and the ACE System of Records Notice (71 FR 3109, dated January 19, 2006).

With respect to mail importations there are similarly no opportunities to decline providing information. Advance collection of this information is mandated by section 343 of the Trade Act of 2002 (Public Law 107-210).

2.2 What opportunities do individuals have to consent to particular uses of the information?

There are no opportunities for individuals to consent to particular uses of information, unless they choose not to create an account, or cross the country's borders, or receive international mail or packages.

2.3 How do individuals grant consent concerning how their information will be used or shared?

Since the program and the requirement to file a Customs Declaration and electronic manifest are mandatory, individuals do not have the opportunity to grant consent concerning how their information will be used or shared. Once an individual's information is provided by the individual or the carrier who employs the individual, it is used to fulfill CBP's statutory and regulatory mandates as defined in this and other CBP systems PIA documentation. The information may also be used by other PGAs with compatible statutory and regulatory mandates as provided for within the terms of a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) executed by both CBP and the PGA. Each PGA and CBP are equally obligated to protect individual privacy rights. FMCSA's Privacy Impact Assessment for the ACE/ITDS FMCSA Pilot, will be posted on the DOT web site. .

2.4 What are the procedures for individuals to gain access to their own information?

Account holders may access their own account information at any time. Individuals such as drivers who wish to view their information in ACE must gain access through the company that employs them. If an individual holds a FAST Driver Proximity Card, then the individual may gain access in accordance with those rules.

2.5 What are the procedures for correcting erroneous information?

There are four methods employed to enter personal data into the ACE system and four separate procedures to correct erroneous information.

- **Information input into ACE Accounts by account holders**

  Account holders may correct erroneous information by logging into their account and changing the information. Individuals such as drivers and crew members may correct information by requesting that the account holder that employs them update the data. A CBP Officer cannot change any information stored in the account holder's account itself.

- **e-Manifest information entered on a one time basis by account holders**

  At the point of entry, if it is determine the e-Manifest information is incorrect, a CBP Officer can put a note in ACE to indicate incorrect personal information is in an e-Manifest related to the crew, conveyance, and equipment. An upcoming ACE release will allow a CBP Officer to change a crewmember's name or date of birth on the e-Manifest itself.

- **FAST Driver account information for e-Manifests**

  As described above, FAST system data will populate an e-Manifest if the driver or crewmember has a FAST Driver Proximity Card. An individual with a FAST driver account can change erroneous personal information at any FAST enrollment system. Refer to Section IV, Data Access, of this document for more information.

- **Information placed in ACE Accounts by Data Transmission from USPS**

Account holders, who have obtained access to ACE via the internet, through a secure data portal, may correct erroneous information by logging into their account and changing the information. Individuals without this Secure Data Portal Access or direct system-to-system access must file a request with the Customer Satisfaction Unit.

As an example: a truck driver arrives and his/her date of birth is listed as 08/12/1957 on the electronic truck manifest. A CBP Officer in the primary booth asks the driver for his driver's license and notices that the date of birth on this document is 12/08/57. In this example, unless the CBP Officer uses the correct date of birth, screening will not be run on the actual person sitting in the truck. The ACE Release 4 provides the CBP Officer in the Primary Booth the ability to document this change in the record and run screening on the correct person. This change/correction never changes the electronic truck manifest submitted by the account holder, but it will be noted in the system. The type of change/correction can also be accomplished with the other personal information concerning driver/crew member(s). CBP Officers can never change shipment information.

If the above mechanisms do not address the concerns of the individual, CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems. Inquiries to the Customer Satisfaction Unit should be addressed to: **Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229 (phone: (202) 344-1850 and fax: (202) 344-2791 service are also available)**. Individuals making inquiries should provide as much identifying information as possible to identify the record at issue.

If an individual has a question regarding the information in the system about him/her while at the border, the CBP Officer will provide the individual with the appropriate fact sheet. If the problem involves the Interagency Border Inspection System (IBIS), the IBIS fact sheet will be provided. If the problem is incorrect carrier or FAST information, an ACE fact sheet will be provided.

Section Three: Data Access

3.1 Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others) and is it documented?

Direct system access will be given to participating truck carriers and their authorized agents, customhouse brokers, importers, CBP employees, and employees of PGAs where the PGA and CBP have executed the necessary MOA. Data access rights are documented in ACE system security documentation. Trade community users have access only to their own account data. CBP users have access to the data deemed necessary by their user role. The access levels are explained in the ACE system documentation.

3.2 How will access to the data by a user be determined?

Data access is determined by permission levels. Users have certain rights based on account type. The ACE/ITDS users will enter via a Web Portal, which will allow users access based on their role and profile. The PGA users, entering either via a Web Portal or by means of direct system access, will be required to authenticate with a unique ID and password. User access is controlled by access control decisions that are made based on user system security attributes (e.g., assignments to groups, which are group IDs based on the specific role). System security policy guidelines are provided for the creation of secure passwords and must be adhered to by the PGAs.

3.3 Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes. Access is strictly controlled and documented in the ACE system documentation.

3.4 Will users have role-based access to data on the system limiting them to some but not all of the data?

Yes. ACE user role-based access is restricted in the form of Mandatory Access Controls. This means that users cannot assign their roles to any other user, nor can they elevate their rights within the system. User access is enforced with documented ACE security procedures.

3.5 What controls are in place to prevent the misuse (e.g., browsing, expired privileges, etc.) of data by those having access?

ACE has the ability to track or audit what a user is doing. This system auditing provides a mechanism to ensure that users can be held accountable for their actions. The system maintains a record of the functions performed, files accessed, and information entered or modified.

The primary goal of security auditing and logging is to record information about potential security incidents for subsequent analysis and to provide forensic evidence of security incidents. The ACE auditing feature provides the capability to track all users' activities within ACE from end-to-end.

Data integrity controls are used to protect data from accidental or malicious alteration or destruction, and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls are used to determine compliance with security specifications and requirements.

3.6 Do other systems share data or have access to data in this system? If yes, explain. Include a discussion of who will be responsible for protecting the privacy rights of individuals affected by the interface.

Yes. e-Manifest data from ACE will be transmitted to several CBP systems and, at this time, one PGA, the FMCSA. Pre-filed information in the e-Manifest allows ACE to screen the information before the truck arrives at the border. ACE will display the data in Current systems *i.e.*, the systems listed below and ACE data in one easy-to-use CBP Officer portal screen, giving CBP Officers a comprehensive view of enforcement and transaction history data.

The following CBP systems receive e-Manifest information from ACE:

- **Automated Commercial System – ACS**

The ACS is a highly integrated computer environment that uses a central processing system and a central database to track, control, and process all goods imported into the United States. The only personal information transmitted to ACS is the driver's FAST Driver Proximity Card number, if applicable.

- **Automated Targeting System – ATS**

The ATS is a decision, support, and analysis tool. A rule-based system, ATS uses electronically filed shipment data to search for criteria that could indicate high-risk cargo. e-Manifest information is sent to this system. The ATS system is not used to validate personal information collected by ACE, but is under development to do so in future Screening and Targeting ACE releases. This PIA will be updated and released to the public before these planned releases are conducted.

- **Free and Secure Trade – FAST**

FAST facilitates the flow of information within CBP, the trade community, other government agencies, and foreign governments. The system leverages pre-filed entry data, including conveyance and cargo information. The pre-filed entry data triggers a recommended electronic pre-release, since entries are transmitted to CBP before cargo arrives at the border. FAST sends a list

of all registered drivers to ACE and ACE stores this information in the system. FAST data within ACE is updated every 30 minutes. After an application, vetting, and interview process, a driver can obtain their FAST Driver Proximity Card at a FAST Enrollment Center. If errors are noted in the FAST system, the driver data can be updated by the driver at a FAST enrollment center.

- **Treasury Enforcement Communications System (TECS)/IBIS**

TECS is a law enforcement system that ACE uses to validate the admissibility of crewmembers and passengers. The ACE data is not used to update this system.

- **FMCSA's System**

E-Manifest information is submitted by the carriers to CBP. Subsequently, the data elements pertinent to FMCSA will be verified by FMCSA's Query Central, a clearinghouse database, which will interface with other FMCSA systems. For more information on FMCSA's processes and systems, see FMCSA's separate Privacy Impact Assessment, available on DOT's web-site.

3.7 Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

The personal data that will be transferred to FMCSA for verification against identical information already collected by FMCSA and the identification of inconsistent information is as follows: 1) ACE User ID 2) CDL number 3) CDL state 4) CDL country 5) CDL last name 6) CDL first name 7) Commercial driver's date of birth. This information is collected from the e-Manifest submitted by the carriers to CBP. After the information is collected from the e-Manifest, the data elements pertinent to FMCSA will be verified via FMCSA's Query Central, a clearinghouse database, which will interface with other FMCSA systems. For more information on FMCSA's processes and systems, see FMCSA's separate Privacy Impact Assessment, available on the DOT web-site.

3.8 How will the data be used by these other agencies?

The FMCSA has been given the responsibility to reduce crashes, injuries, and fatalities involving large trucks and buses and already collects the subject data under its own authority and means. FMCSA will use the data from ACE to verify information existing in its system and will benefit from CBP checking this information at the border and prior to border crossing. All of this will help FMCSA in carrying out its safety mandate.

3.9 Who is responsible for ensuring proper use of the data by other agencies?

Participation in ACE/ITDS will be governed by an MOU between CBP and the respective PGA, in this first instance, FMCSA. For example, The ACE/ITDS FMCSA Pilot will not become operational prior to the establishment of such an MOU. CBP is responsible for sharing only the data required by MOU, and FMCSA is responsible for using the data in accordance with the MOU.

3.10 How will the system ensure that other agencies only get the information they are entitled to?

Users are granted limited roles with access to specific portions of ACE after approval from a CBP program officer and evaluation by CBP's Information Systems Security Branch (ISSB). Only the data covered by the MOU will be transmitted to PGA, such as FMCSA, or made available to a PGA through its Web Portal. PGAs such as the FMCSA will have no access to data not covered by their respective MOUs.

Section Four: Maintenance & Administrative Controls

4.1 Is the data secured consistent with agency requirements under the Federal Information Security Management Act?

The ACE project is required to follow the Customs Systems Development Life Cycle (SDLC) (CIS HB 5500-7A) that requires each system to be certified and accredited. The SDLC is developed from the Government Information Security Reform Act (GISRA), which is now known as the Federal Information Security Management Act of 2002 (FISMA), and National Institute of Standards and Technology (NIST) guidance and must be included as part of the certification and accreditation process. The security requirements outlined in the SDLC have to be satisfied at the appropriate project development stage before it can move toward a subsequent development stage.

In addition, each project is assigned with a team of the technology subject matter experts, including at a minimum of a network/systems engineer, a System Design Security Officer (SDSO) and a Computer Security Officer (CSO), who work collaboratively to achieve the following: 1) Site survey (if the site involved, where system/application would be set up) to perform physical security risk assessment to ensure adequate physical security provided for the site and 2) Vulnerability assessment of the system/application (including cabling, wide area network circuits, servers, network-connected devices, secure racks, personal computers, and software) to ensure that vulnerabilities are identified and corrected prior to the certification & accreditation and operation of the site and its system/application.

The ACE is being developed using well-established security architecture principles that include 1) defense-in-depth, 2) layered defenses, and 3) multi-tiered security architecture. The security capabilities provided in the database system include user account validation, user profile management, database object access control, and audit trail.

The ACE security infrastructure is based on the National Security Agency's Defense-in-Depth strategy, which is a practical strategy for achieving information assurance in today's highly networked environments. The defense-in-depth strategy is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The basic security goals for ACE are to protect the different sub-systems from any potential security risks, actively defend against attacks, detect any security breach regardless of when or where it occurs, and be ready to respond to all security incidents.

The ACE implementation of security is compliant with the data security measures defined by CBP Infrastructure Services Division (ISD), ISSB, to protect such data, including identifying the requirements for physical protection and storage of the data. This includes compliance with ACE Security Plans, ACE Security Design, and the *U.S. Customs Service Information Systems Security Policy and Procedures Handbook, HB CIS 1400 05A*, dated June 22, 2001.

The ACE implementation supports awareness of security breaches and potential data compromise. Appropriate security monitoring and planning–including an analysis of risk and contingencies and the implementation of appropriate contingency plans, as required by Presidential Decision Directive-63 (PDD-63), have been carried out to prevent unauthorized access to ACE information.

Each individual with access to ACE is responsible for protecting CBP data and for maintaining good order during day-to-day operations. Controls within ACE ensure that each user is accountable for his/her own actions and protect data from malicious or accidental damage or loss.

Access to the computer area is controlled by a security pass arrangement and personnel not connected with the operation of the computer are prohibited from entering. A uniformed guard protects building security. Access at the ports is from the booths and from any PC connected to the Local Area Network (LAN). At the ports of processing, terminal rooms are under close supervision during working

hours and locked after close of business. The system security officer issues a unique private five-digit identification code to each authorized user. Access to CBP computers from other than system terminals is controlled through a security software package. Users must input a unique identification code and password during the terminal login procedure to gain access to the system. The password is not printed or displayed at the port of processing. The system validates the user ID by transaction type, thereby limiting a system user's access to information on a ``need-to-know'' basis. A listing of identification codes of authorized users can be printed only by request of the security officer. The passwords are changed periodically to enhance security processing.

4.2 Affirm the agency is following information technology security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

CBP ensures the handling of personal information is consistent with government policies through the enforcement of the policies and procedures documented in CIS HB 1400-05A, which complies with federal policies and guidelines.

The ACE functional security requirements are derived primarily from DHS, Information Technology Security Program Publication MD-4300A, Policy Guide for Sensitive Systems, dated June 1, 2003, and CBP, Information Systems Security Policy and Procedures Handbook (CBP HB 1400-05A), June 22, 2001. Those requirements are separated into eight distinctive areas: 1) Administrative/Management Security, 2) Communications Security, 3) Computer Security, 4) Contingency Planning, 5) Information Security, 6) Personnel Security, 7) Physical Security, and 8) DHS-specific Auditing Requirements (as per DHS MD-4300A).

4.3 Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.

An ACE Security Risk Assessment was developed and completed on August 23, 2002 in compliance with FISMA, Office of Management and Budget policy, and NIST guidance. Security risk assessment and tests were conducted for subsequent releases: ACE Release 3 in June 2004 and ACE Release 4 in December 2004.

4.4 Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly to safeguard system data.

The management, operational, and technical security controls were tested for effectiveness and are reevaluated when new ACE releases are conducted.

4.5 Provide a point of contact for any additional questions from users.

Contact the Customs and Border Protection Modernization Office with any additional questions. Refer to Section VII, Privacy Risk Analysis, of this document for contact information.

4.6 If the system is operated in more that one site, how will consistent use of the system and data be maintained in all sites?

Application data is maintained at CBP National Data Center (NDC) site. This means that one location "controls" the data and there is no duplication of information. All ACE users undergo training on the ACE system before they are allowed access to ensure proper use of the system and data.

4.7 What are the retention periods of data in the system?

Personal information collected in ACE as part of the regulation of incoming cargo and people will be retained in accordance with the U.S. Customs Records Schedules approved by the National Archive and Records Administration for the forms on which the data is submitted. This means that cargo, crew, driver, and passenger information collected from a manifest presented in connection with the arrival of a vessel, vehicle or aircraft will be retained for six years. Information collected in connection with the submission of a Postal Declaration for a mail importation will be retained for a maximum of six years and three months. Lastly, information pertaining to CBP and PGA employees will be retained for as long as the individual maintains her or his portal access to ACE.

With respect to information collected by ACE, shared, and maintained within other CBP or PGA systems, that information will be retained by the those systems in accordance with the approved record retention schedules for each respective system. For a further discussion of ACE's interaction with other CBP systems and PGA systems, please refer back to section IV. Data Access.

4.8 What are the procedures for expunging the data at the end of the retention period and are these procedures documented?

Records identified for destruction in accordance with the U.S. Customs Records Schedule will be deleted, erased, scrubbed or subject to other suitable means of permanent destruction in an electronic environment.

Additionally with respect to issues regarding redress, CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems (including ACE). If the importer, exporter, crew member, driver, passenger, or other person associated with the movement of cargo or passengers across the border believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to the Customer Satisfaction Unit at the following address: Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229 (phone: (202) 344-1850 and fax: (202) 344-2791 service are also available). Individuals making inquiries should provide as much identifying information as possible regarding themselves, to identify the record at issue. Individuals may provide additional information to CBP to ensure that the information maintained by CBP is accurate and complete. The Customer Satisfaction Unit will respond in writing to each inquiry.

The DHS Chief Privacy Officer will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout the process. The DHS Chief Privacy Officer will also serve as the final review authority for all individual complaints and concerns about the program.

4.9 Will the system provide the capability to monitor individuals or groups of individuals? If yes, explain?

There are flexible reporting capabilities in ACE that allow CBP Officers to run reports against system data, such as: all truck drivers employed by a certain account holder. Although the ACE system allows basic ad hoc reporting, at this point in system development, screening and targeting activities are not performed in ACE itself.

4.10 What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

To prevent unauthorized monitoring, trade community users may only access their own account data. CBP employees with access to ACE are restricted to only the data they need according to their defined

user type, or profile. These employees have a demonstrated need to use the system, have undergone training, and have security clearances granted based upon the successful completion of a background investigation. User Provisioning assigns ACE users appropriate user profiles and credentials and distributes them to the ACE system components that need them. The ACE employs a role-based user provisioning process that defines business roles and a set of privileges for each role.

4.11 Under which SORN does the system operate? Provide Number and Name.

A SORN for ACE has been published separately (71 FR 3109, dated January 19, 2006) as **DHS/CBP-001, Automated Commercial System/International Trade Data System (ACE/ITDS).**

Section Five: Decision Analysis

5.1 Did you evaluate competing technologies on their privacy handling capabilities? If yes, explain.

No competing technologies were evaluated for privacy handling capabilities. CBP limits and restricts access to information based upon user roles.

5.2 Were any choice changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA? If yes, explain.

No choice changes to system architecture, hardware, or software were made. Choice changes relating to implementation plans, however, were made to inform the public with respect to the submission and handling of their personal data. The system development plan for ACE includes recurring input from both the trade community/public and PGAs as part of a public-private partnership to develop the system and identify the data elements to be collected, either pursuant to a statutory mandate or to permit more efficient business operations for both CBP and the trade community.

Section Five: Privacy Risk Analysis

In analyzing what might constitute risks to an individual's privacy, CBP determined and resolved the following risks:

The reporting of personal information to CBP by ACE account holders:

Previously, CBP did not request that account holders inform their employees that their personal information was being reported to ACE. CBP included language in Federal Register Notices and CBP's ACE Privacy Policy to strongly encourage ACE account holders to inform their employees of any personal information reported to ACE.

Updating inaccurate personal information in ACE:

The ACE system must allow individuals to update erroneous information and CBP has developed a specific process to allow for this, as individuals do not know personal information recorded in ACE is incorrect until a CBP Officer processing their arrival alerts them. CBP has developed an ACE Fact Sheet (*see*, Appendix) to assist a CBP Officer in quickly and effectively communicating 1) what personal information is incorrect in the ACE system and 2) how the information may be corrected. If a CBP Officer discovers erroneous information in the ACE system, the ACE Fact Sheet will be given to the individual during the border crossing transaction. With the information provided in this fact sheet, the individual may then seek

redress from the Customer Satisfaction Unit to correct or amend the particular data identified as being erroneous.

For questions or comments, please contact:

Laurence Castelli
Chief, Privacy Act Policy and Procedures Branch, Office of Rulings and Regulations / Office of Information Technology
Customs and Border Protection
(202) 572-8712

Appendix

1. ACE Fact Sheet

ACE FACT SHEET

What is ACE?
ACE is the acronym for the Automated Commercial Environment.

Who Uses ACE?
In addition to U.S. Customs and Border Protection (CBP), other Participating Government Agencies (PGAs) of the Federal government will have access to the information collected by ACE through the International Trade Data System (ITDS). Individual account holders may also access their own information as well.

What does ACE Provide?
ACE provides the participating account holders the ability to monitor the status of their transactions with CBP and other PGAs, as well as allow for trend analysis, internal auditing, and compliance based upon the use of historical records of recent transactions. ACE, through ITDS, provides CBP and other PGAs the ability to monitor and analyze the passage of commodities, materials, and persons involved in global commerce before the truck arrives at the border.

Where is ACE?
ACE uses the International Trade Data System as an interface, which allows for secure, integrated, government-wide sharing of the information that has been collected. The users at the PGAs will query the information that is pertinent to their offices independently through the ACE/ITDS interface. Field level access is provided in the CBP Officer portal screen located at the land ports of entry, as well as at system terminals located throughout the processing ports. ACE is a national information system and database maintained and located within CBP, at its National Data Center, to provide support for CBP's Trade Facilitation mission.

What information is in ACE?
ACE keeps track of information on the individuals, businesses, brokers, and vehicles involved in transporting goods across international borders. This information includes such things as truck carrier, broker, and importer account information, as well as information collected through electronic truck manifests (e-Manifests) submitted by the participating carriers. ACE cross-references the e-Manifests with information obtained from the Federal Motor Carrier Safety Administration (FMCSA) to verify that data is current and consistent. The information is used to assist CBP and PGAs in regulating and monitoring international trade related activities, as well as ensuring individual compliance with rules and regulations.

Customs and Border Protection's (CBP) collection of driver/crew/passenger information.
CBP has the authority to collect information on all persons entering or leaving the United States. This information is used for purposes related to streamlining CBP business processes, facilitating growth in trade, and ensuring the safety and security of our borders.

Additional Questions or Clarifications?
Discrepancies relating to information in ACE relating to a person's Name, Address, or Date of Birth, may be addressed at the time of crossing the border. Any other clarifications to information collected from or about you and any concerns you may have as an international transporter or traveler about the use or application of ACE and its impact on you may be addressed to:

U.S. Customs and Border Protection

Customer Satisfaction Unit, Office of Field Operations
Room 5.5 C
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229

Please ensure that you provide a sufficient amount of personal identifying information (**legible** copy of your passport, driver's license, etc.) for CBP to perform an in-depth inquiry into your concerns.

June 2006