

**Customs Process Automation (CPA)
Privacy Impact Assessment (PIA)**

1. Department of Defense (DOD) Component:
United States Transportation Command (USTRANSCOM)
2. Name of Information Technology (IT) System
Customs Process Automation (CPA)
3. Budget System Identification Number (SNAP-IT Initiative Number):
1137
4. System Identification Number:
490
5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable):
007-97-01-03-02-1137-00-118-060
6. Privacy Act System of Records Notice Identifier (if applicable):
N/A
7. OMB Information Collection Requirement Number (if applicable) and Expiration Date:
N/A
8. Type of Authority to collect information (statutory or otherwise):
Statutory: Title 5 United States Code, Section 301; (Title 10 United States Code, Section 164)
DOD Regulation: Defense Transportation Regulation (DTR) DODR 4500.9-R-Part V
9. Provide a brief summary or overview of the IT system that includes at minimum: activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup procedures.

ACTIVITY/PURPOSE: CPA will provide automated processing of customs documents for duty free entry of Department of Defense (DOD) cargo into host nations where DOD forces operate. DOD cargo includes general cargo, household goods, privately owned vehicles, and unaccompanied baggage. Automating the customs and border clearance process will reduce transit times and provide more efficient and streamlined processing for cargo. Services and Combatant Commands (COCOMs) will benefit from faster delivery, reduced costs and reduced frustrated cargo.

CURRENT LIFE-CYCLE PHASE: CPA is presently in the development and demonstration phase with all its resources provided by USTRANSCOM.

SYSTEM OWNER: The system owner is United States Transportation Command (USTRANSCOM).

SYSTEM BOUNDRIES AND INTERCONNECTIONS: CPA will consist of a suite of servers in a tiered environment. The primary web server is accessed from the internet via Secure Socket Layer (SSL). The CPA web server, database server, application server, and backup servers will be hosted in one of Defense Information Systems Agency (DISA's) Defense Enterprise Computing Centers (DECCs). The location of CPA and its components will be

Customs Process Automation (CPA) Privacy Impact Assessment (PIA)

behind a firewall at the DISA DECC facility in Mechanicsburg, PA. CPA receives transportation-related data from other transportation systems via feeds which are secure.

LOCATION OF SYSTEM AND COMPONENTS: The Primary Servers and Test Environment are at DECC Mechanicsburg

SYSTEM BACKUP: The system backup is a part of the normal system maintenance with the database backed up on a reoccurring basis and incremental backups occurring daily.

10. Describe what personal information will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DOD, etc...). Describe the covered individuals (i.e., individuals whose information will be collected — military, civilian, public, etc...). Estimate the number of individuals whose Personally Identifiable Information (PII) is (will be) collected. If a system collects PII on more than 500 personnel in a single device or is accessible through a single application or service, the system must be treated as a High Impact PII Category system. The PMO of such a system is responsible for implementing additional protection measures.

CPA will collect Identification Information, such as First Name, Last Name, Rank, SSAN, Middle Initial, Pay grade, travel order number, Contact Information, such as Business Address, Business Phone Number, Business FAX Number, Business E-mail and Customs Approval Authority Information, such as Seal Number and Stamp Number. The source of this information will be a data interface with the Defense Personal Property System (DPS), commercial carrier systems (foreign and US), manual entry of data through customs forms, and manual entry of data to create CPA accounts. Military, DOD-civilians, and foreign and US contractor information is collected in order to complete customs procedures. The estimated number of individuals is well over 500 since movement of all DOD personnel overseas uses the customs process. CPA will implement the access/authorization controls to protect privacy data.

11. Describe how the personal information will be collected (e.g., via the Web, via paper-based collection, etc...). Describe the controls that are in place to ensure the information is accurate upon entry and during use. Describe the opportunities individuals have to access and/or correct information about them. Identify the risk inaccurate information poses to the individuals and what is being done to mitigate the risk.

PII will be collected via Web input by users of the system. Personal information will also be collected from a data interface with the Defense Personal Property System (DPS) via Secure connection, manual entry of data through customs forms, and manual entry of data to create CPA accounts where PII is required for shipments. Access to the system will be PKI-based requiring a DOD approved certificate, such as common access card or external certification authority (ECA) approved vendor certificates and password/UserId when DOD Approved certification cannot be obtained. Individuals will be able to access their CPA system account information and update it as required through a secure web-based interface. CPA will implement JTF/GNO guidance. Inaccurate information may cause shipment delays. Information is verified during entry to the DPS system and remains untouched in CPA. It is only used as source information.

12. Describe the requirements and why the personal information is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc...). Then, explain why this

Customs Process Automation (CPA) Privacy Impact Assessment (PIA)

is the minimal information needed to support the system. Identify the risk posed to the individuals should there be unauthorized access to this information and what is being done to mitigate the risk.

Personal information is collected to provide automated processing of customs documents for duty free entry of Department of Defense (DOD) cargo into host nations where DOD forces operate. Once personal information is received, it will be stored at a DISA DECC facility with restricted access. The information is required by host nations for customs clearances. Host nations could be any nation that the United States has a status of forces agreement (SOFA) negotiated. The personal information is collected to verify the trustworthiness of individuals requesting access to DOD information, sensitive and unclassified and to meet the minimum security standards for access to a DOD information technology system. Identifiable information must be collected to execute the USTRANSCOM missions for moving personal property in accordance with DOD 4500.9-R, Part IV, Personal Property Movement. The minimal personal information stored in the system that could be compromised is the users name, social security number (embedded in the Transportation Control Number (TCN)), email address, phone number, organization, and password. This unique number is composed from known information (such as social security number, shipping number, date, etc). The risk posed to the personal information collected is minimal because all user personal information is encrypted; site resides behind a firewall; users do not have the ability to view other user's information; and site administrative, physical, and need-to-know security requirements protect both user and cargo information. CPA account managers must collect identifiable information to accommodate security regulations/directives to uniquely identify users who want an account. Appropriate user access allows the user to execute customs activities.

13. Describe how the personal information will be used (e.g., to verify existing data, etc...). Describe how long the information is retained, why it is needed for that length of period, and how it is destroyed. Describe any risks associated with retention and their mitigation effort.

CPA's use of personal information is described in paragraph 12 above. Maintain customs clearance transactions on-line for a period of seven years, then archive to magnetic media. The period of archive is 10 years for documents associated with a normal shipment. During a period of war, documents associated with shipments entering or departing the war zone must be archived until such time the war is declared over, after which these documents will be held for an additional 10 years. Archive is established per request by host nations participating in the program and by Defense Transportation Regulations. Risk associated with retention is limited to accessibility of the on-line archive. On-line archive is only accessible by PKI-pin login. Magnetic media tapes will be degaussed.

14. Describe whether the system derives or creates new data about individuals independently or through aggregation and what controls are in place to ensure the information is accurate.

The system does not derive or create new data about individuals independently or through aggregation.

Customs Process Automation (CPA) Privacy Impact Assessment (PIA)

15. Describe with whom the personal information will be shared, both within the Component and outside the Component (e.g., other DOD Components, Federal agencies, etc.). Also, explain the purpose for sharing the personal information, how the information is shared, the controls that are used to protect the information during transmission, and the formal agreements that exist to ensure the shared information is handled appropriately by the other party.

Personal information will be shared with individuals involved in the customs clearance process. These individuals include DOD Customs Clearance Officers, commercial carrier port agents, and Host Nation customs agents. Command and control personnel (USTRANSCOM, COCOMs, and Army Air Force Exchange Service and the Defense Logistics Agency will also be able to view personal information. The personal information will be shared by displaying the information, along with other relevant shipment information, via the Web pages of the CPA system. Furthermore, when hard copy customs documentation is required, the personal information will be printed as required. Personal information in the CPA system will not be supplied to other systems. Personal information is required to clear shipments for duty free entry into Host Nations where the DOD operates. Personal information will predominantly be used for personal property shipments. Personal information displayed on CPA system Web pages will be passed on the Internet and NIPERNET via SSL security controls.

16. Describe any opportunities individuals will have to object to the collection of personal information about them to decline to provide information and the consequences thereof, or to consent to the specific uses of the personal information. If applicable, describe the process regarding how the individual is to grant consent or how the individual can decline to provide information.

Personnel associated with DOD are provided Privacy Act Statements and opportunities to decline to provide data. Since privacy data is used to identify certain shipments (i.e., household goods and privately owned vehicle shipments). Originating systems afford the individual the opportunity to grant consent or decline to provide information. The account creation process necessitates some personal information and privacy act statements will be provided. Failure to provide personal information for account creation purposes may result in denial of an account.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect or handling of the PII.

PII will be collected in electronic form through either the individual entering data into forms during account creation, the individual entering data into forms during self-counseling for personal property, or the information being entered by a personal property shipment officer during face-to-face counseling. Privacy Act Statements and advisories will be on the forms requiring PII and presented on the screen during account creation.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the personal information.

Administrative/business processes and controls-

Customs Process Automation (CPA) Privacy Impact Assessment (PIA)

Processes and procedures such as configuration management, disaster recovery, etc. have been implemented and documented. Additionally, system administrators and network management personnel are located at and provided by the DECC at Mechanicsburg, PA and are governed by IA guidance, policies and procedures implemented by the DECC. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know.

Physical processes and controls-

The CPA is hosted at the DISA DECC in Mechanicsburg, PA and will inherit the physical security protection mechanisms already in place. The DISA DECC Security Manager or top-level manager responsible for each site is responsible for its physical security. Physical security measures must meet the following objectives:

- Safeguard personnel
- Prevent unauthorized access to equipment, facilities, material, media and documents
- Safeguard against espionage, sabotage, damage and theft
- Reduce the exposure to threats that could cause a denial of service or unauthorized alteration of data.

Entry to the building is controlled by a card reader system. During normal duty hours, visitors are controlled by a person posted in the lobby. There are nine entry/exit points. All are locked and/or controlled. Entry is also controlled for computer rooms. Building is a one-story structure. There are nine entry/exit points. All are locked and/or controlled. The facility uses commercial power. In the event of a commercial power failure, the building can operate by using the Uninterruptible Power Source (UPS), supplemented by backup generators, which ensures continued operation.

Technical processes and controls-

All Web transactions will be encrypted over SSL through identification and authentication of each user. Audit will allow the system to collect and maintain information used to monitor security-relevant system use and investigate possible attempts to breach the system.

Discretionary access control will allow users access to information according to the user's identity. Object reuse will prevent one user from obtaining another's residual data. DISA will be responsible for network security by providing, configuring, and maintaining the intrusion detection system (IDS) for CPA. DISA will also be responsible for the implementation of access control lists (ACL) on DISA routers to provide security for CPA.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DOD Directive 5400.11, "DOD Privacy Program," 8 May 2007 and DOD 5400.11-R. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

The System of Records notice is not required. CPA is not the source of any privacy act information. All information is received by interfaces with originating systems.

**Customs Process Automation (CPA)
Privacy Impact Assessment (PIA)**

20. Describe/evaluate further any risks posed by the adopted security measures (i.e., Design choices that were made in order to mitigate privacy risk; security measures to mitigate privacy risks due to providing individuals an opportunity to object/consent or notify individuals; etc...).

Design considerations took into account protection of Privacy Act data as did the choice of locations for data storage. Records will be maintained in a DISA secure data facility and is accessible only to authorized personnel. All data is encrypted during transmission. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by PKI, PIN protected.

21. State classification of information/system (Sensitive or Public) and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, it should be published in a summary form.

The system is Unclassified but considered Sensitive and operates on the Non-Classified Internet Protocol Router Network. This version of CPA PIA will be published in its full form upon approval by the USTRANSCOM Approving Official.

Preparing Official: ___(Original Signed 7 Feb 08)___

Name: Mr. Paul Jones

Title: Deputy Program Manager, Customs Process Automation

Organization: USTRANSCOM/TCJ6P

Work Phone Number: DSN 576-6525, COMM: 618-229-6525

Email: paul.jones@ustranscom.mil

**Customs Process Automation (CPA)
Privacy Impact Assessment (PIA)**

Information Assurance Official: __ (Original Signed 8 Feb 08) __

Name: William Hedgecough

Title: Senior Information Assurance Officer

Organization: United States Transportation Command

Work Phone Number: (618) 229-4049

Email: tcj6-oip.@ustranscom.mil

Privacy Official: __ (Original Signed 10 Mar 08) __

Name: JoLynn Bien

Title: Privacy Act Officer

Organization: United States Transportation Command

Work Phone Number: (618) 229-3828

Email: ustccs-im@ustranscom.mil

Legal Official: __ (Original Signed 7 Mar 08) __

Name: Ronald J. Williams, Colonel, USAF

Title: Staff Judge Advocate

Organization: United States Transportation Command

Work Phone Number: (618) 229-1366

Email: ustcja@ustranscom.mil

Reviewing/Approving Official: __ (Original Signed 11 Mar 08) __

Name: DANIEL R. DINKINS, JR., Brigadier General, USAF

Title: CIO, United States Transportation Command

Organization: United States Transportation Command

Work Phone Number: (618) 229-3824

Email: ustc-egov@ustranscom.mil