U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT

Name of Project:	International Trade Data System/Risk Assessment Methodology (ITDS/RAM)
Office/Directorate:	Office of Import Surveillance and Inspection/Safety Operations

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	Ken Asher, Consultant, Information Technology Policy and Planning (ITPP), 703 887-6455
System Owner: (Name, title, organization and ext.)	Carol Cave, Director, Office of Import Surveillance and Inspection, 301-504-7677
System Manager: (Name, title, organization and ext.)	John Blachere, International Trade Specialist, Office of Import Surveillance and Inspection, 301-504-7996

B. APPROVING OFFICIALS

	Signature	Approve	Disapprove	Date
System Owner Carol Cave, EXIS	9/22/2011 X Carol Cave Carol Cave Director, Office of Import Surveillance and Ins...			
Privacy Advocate Linda Glatz, ITPP	9/22/2011 X Linda Glatz Linda Glatz			
Chief Information Security Officer Patrick Manley, ITTS	9/27/2011 X Patrick Manley Patrick Manley			
Senior Agency Official for Privacy Mary James, Director, ITPP **System of Record?** __X__ **Yes** ____ **No**	9/29/2011 X Mary James Mary James			
Reviewing Official: Patrick D. Weddle, AED, EXIT	9/29/2011 X Patrick D. Weddle Pactrick D. Weddle			

C. SYSTEM APPLICATION/GENERAL INFORMATION

1. Does this system contain any personal information about individuals? (If there is **NO** information collected, maintained, or used that is identifiable to the individual, the remainder of PIA does not have to be completed.)	Yes, The system contains Names and Social Security Numbers associated with individuals and small businesses importing materials into the United States. Information on individuals is only stored when they register as the entity in the transaction, usually, this is a business entity instead with associated Importer Number and business addresses.
2. Is this an electronic system?	Yes

D. DATA IN THE SYSTEM	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Public businesses
2. Generally describe what data/information will be collected in the system.	Names, Social Security numbers, Harmonized Tariff Codes, port of entry, customs filer name and address and other items relevant to imported goods.
3. Is the source of the information from the individual or is it taken from another source? If not directly from individual, then what other source?	Information is taken from Import forms Customs and Border Protection (CBP) 3461 and CBP 7501 filed in accordance with United States Law. The 3461 contains items or item groups Declared for entry into U.S. commerce by an importer or a Customs Broker. The 7501 contains Entry Summary Data including estimated duties, taxes, and fees filed by an importer or Customs Broker
4. How will data be checked for completeness?	Data will not be checked for accuracy.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Data is provided by the Importer. It is not checked for currency.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	Yes, data is described in CBP Documentation for the CBP 3465 and CBP 7501
E. ATTRIBUTES OF THE DATA	
1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?	The data is used to screen imports into the United States to prevent importation of hazardous products.
2. For electronic systems, if the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Explain.	Data is presented in the form of a list of imported items on a daily basis. The data is secured and is only accessible by CPSC employees and contractors with a current Single Scope Background Investigation (SSBI) clearance.
3. How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.	Data can be retrieved using reports by SS# and Name.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	None
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	7 Years per the NARA Records Schedule
2. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?	Data will be destroyed in accordance with the Security Policy and the NARA Records schedule. Data will be retained for 7 years. Procedures will be documented on the ITDA/RAM Production SharePoint site.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No. For a small number of people who choose to identify themselves using their SSN as the importer, they provide an address and name corresponding to that role. In some of these cases, the individual may provide a personal residence. But, as the context of these identifiers are to identify an importer of record for a shipment for legal reasons, we are unable to determine what the address signifies; the address could be for a business. Also, for the vast majority of shipments (>90%), an importer of record

	number (IR#) is the predominant method of identifying a company importing products. In those cases, the address and name associated with this identifier are for a business. Due to the limited use of the SSN in this context, and the unknown nature of the information provided, the use of SSNs in this context cannot be reliably used to identify information about an individual and monitor them.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	System will be secured to using User ID and password to prevent unauthorized access. All CPSC employees and contractors have completed Privacy and Security Training and have signed the Rules of Behavior agreements.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	N/A –This is a new system. There is currently no System of Record Notice.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	The data is secured and is only accessible by CPSC employees and contractors with a current SSBI clearance.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Not available for public release; See Pilot System Access Control Policy Revision: .1 July 12th, 2011
3. Who is responsible for assuring proper use of the data?	Carol Cave – Director EXIS
4. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? Are contractors involved in the collection of the data? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?	Yes, contractors have been involved in the development of the system and will be involved in system operations. No, data will be received via file transfer from Customs and Border Protection daily. Yes, contracts addressed Privacy Act concerns. Privacy Act References: 1. 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a). 2. 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.C.S. 2631). 3. Privacy Act of 1974 (5 U.S.C. 552a) 4. Clause LC 31b - the Contractor agrees that to the extent it collects data on behalf of CPSC, or is given access to, proprietary data, data protected by the Privacy Act of 1974, or other confidential or privileged technical, business, financial, or personal identifying information during performance of this contract, that it shall not disclose such data.
5. Do other systems share data or have access to the data in the system? If yes, explain. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?	No
6. Will other agencies share data or have access to the data in this system? If yes, how will the data be used by the other agency?	No
7. Will any of the personally identifiable information be accessed remotely or physically removed?	Access to the system will be through the CPSC network only from with-in the firewall or remotely via VPN through the CPSC firewall. This is a secure connection and is approved by EXIT management. Data transfer from CBP to CPSC is secured and encrypted in accordance with the Interagency Security Agreement attached.

	Not available for public release; See Interconnection Security Agreement between the U.S. Customs and Border Protection (CBP) and the Consumer Product Safety Commission (CPSC) Automated Targeting System (ATS) and ITDS Risk Assessment Methodology System (ITDS/RAM) Version 1.8 July 12, 2011