

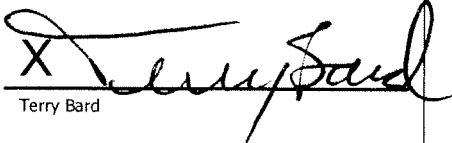

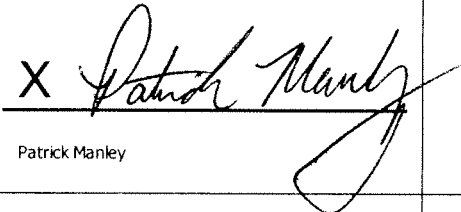
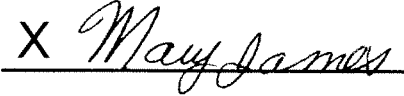
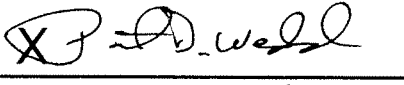
**U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT**

Name of Project: Consumer Product Safety Risk Management System
Office/Directorate: Division of Technology Services

A. CONTACT INFORMATION

Person completing PIA: Patrick Manley, Information Systems Security Officer, ITPP, x6946
 (Name, title, organization and ext.)
System Owner: Terry Bard, Director, Div. of Technology Services
 (Name, title, organization and ext.)
System Manager: Ming Zhu, Branch Chief, Application Development Branch
 (Name, title, organization and ext.)

B. APPROVING OFFICIALS

	Signature	Approve	Disapprove	Date
System Owner Terry Bard, Director ITTS	<input checked="" type="checkbox"/>  Terry Bard	✓		12-22-11
Privacy Advocate Linda Glatz, ITPP	<input checked="" type="checkbox"/>  Linda Glatz	✓		12-22-11
Chief Information Security Officer Patrick Manley, ITTP	<input checked="" type="checkbox"/>  Patrick Manley	✓		
Senior Agency Official for Privacy Mary James, SAOP	<input checked="" type="checkbox"/>  Mary James	✓		
System of Record? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>				
Reviewing Official: Patrick D. Weddle, AED, EXIT	<input checked="" type="checkbox"/>  Patrick D. Weddle	✓		12/21/11

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. System contains Public user's name, birth date, address, email, health data, geographic data, and gender. The system also may include employee name and address.

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 and employees.
2. Generally describe what data/information will be collected in the system.	The CP SRMS data includes consumer incident injury reporting and personal contact data, CPSC manufacturer contact and product data, CPSC statistical data, incident legal case management and litigation data, geographic information associated with incident data, and public affairs data.
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 will primarily be provided by individuals submitting incident reports but also may be provided by CPSC employees, health care providers, hospitals, consumers, local/state/federal government agencies, public safety entities, medical examiners, coroners, and child service providers. Manufacturers/importers/private labelers can provide comments and make claims.
4. How will data be checked for completeness?	CPSC staff does not verify the accuracy, relevance, timeliness, and completeness of the data collected. The submitter has to certify the truth and accuracy of the information submitted. Manufacturers have the opportunity to comment on materially inaccurate information claims. Our disclaimer states "CPSC does not guarantee the accuracy, completeness, or adequacy of the contents of the Publicly Available Consumer Product Safety Information Database on SaferProducts.gov, particularly with respect to information submitted by people outside of CPSC."
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Information is provided by the consumer. 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?)	CP SRMS ODS Data Dictionary.
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 will be used to support the CPSC mission of protecting the public from unreasonable risks of serious injury or death from products such as toys, cribs, power tools, cigarette lighters, and household chemicals that pose a fire, electrical, chemical, or hazard that can lead to consumer injury.
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.	The system has been categorized as a moderate impact system and subject to 18 families of controls identified in the baseline security requirements of Annex 2 of NIST SP 800-53, Recommended Security Controls for Federal Information Systems. Among the controls employed are: strong authentication and authorization, separation of duties, discretionary access controls, encryption of data in transmission, boundary network access controls and intrusion detection, and appropriate disposal of data output.
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.	No. While the incident records may include unique personal identifiers, individual records cannot be retrieved by any unique personal identifier through the application's primary user interface.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Consumer submitting an incident report can decline to have personal information provided to manufacturer.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	Data retention varies depending on the type of record according to the NARA approved CPSC Records Schedule. Monthly system backups of the entire system are created and maintained as permanent records. Some records have a temporary status including:

	<ul style="list-style-type: none"> Hot line call records can be destroyed immediately after being entered or validated in the system. Investigative reports are to be retired to the Washington National Records Center in annual increments when 10 years old and destroyed when 30 years old. Section 15 Case Files are retired to the Washington National Records Center 1 year after file closure and destroyed 15 years after transfer. Legal and Legislative Records are closed annually and retired to the Washington National Records Center 7 years after cut off and destroyed when thirty years old.
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?	Purging of the data must be approved by the system owner, privacy officer, chief information officer and records manager. A formal letter must be written or interagency agreement developed based on the NARA approved record schedule indicating that the data will be transferred to the Washington National Records Center on the agreed upon schedule and upon validation of receipt of the data, the data will be purged from the system of record.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	System will be secured 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 (Not a System of Records).
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	Application users, system administrators, developers.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	CPSC Rules of Behavior, Ethics training
3. Who is responsible for assuring proper use of the data?	The system security organization consisting of the Agency Privacy Officer, Designated Approving Authority, Information System Security Officer and System Owner.
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.
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	Yes, the Centers for Disease Control (CDC), Federal Drug Administration (FDA) and the National Highway Traffic Safety Administration (NHTSA).

system? If yes, how will the data be used by the other agency?	The CDC uses epidemiology data to proactively determine health trends, the FDA and NHTSA use data for ongoing injury studies.
7. Will any of the personally identifiable information be accessed remotely or physically removed?	No.