

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

<b>Name of Project:</b>	CPSC Stakeholders Meeting/New Consumer Product Safety Law			
<b>Office/Directorate:</b>	EXPA			
<b>A. CONTACT INFORMATION</b>				
<b>Person completing PIA:</b> (Name, title, organization and ext.)	Patty Davis, Public Affairs Specialist, EXPA, x7601			
<b>System Owner:</b> (Name, title, organization and ext.)	EXPA			
<b>System Manager:</b> (Name, title, organization and ext.)	EXPA			
<b>B. APPROVING OFFICIALS</b>				
	<b>Signature</b>	<b>Approve</b>	<b>Disapprove</b>	<b>Date</b>
<b>System Owner</b>	Patty Davis, EXPA <i>Patty Davis EXPA</i>	✓		8-15-08
<b>Privacy Advocate</b>	Linda Glatz, ITTP <i>Linda Glatz</i>	✓		8-15-08
<b>Chief Information Security Officer</b>	Patrick Manley, ITTS <i>Patrick Manley</i>	✓		8-15-08
<b>Senior Agency Official for Privacy</b>	Mary Kelsey, Director, ITTP <i>Mary Kelsey</i>	✓		8-18-08
<b>System of Record?</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Mary Kelsey, Director, ITTP	✓		8-18-08
<b>Reviewing Official:</b>	Patrick D. Weddle, AED, EXIT <i>P.D. Weddle</i>	✓		8/15/08
<b>C. SYSTEM APPLICATION/GENERAL INFORMATION</b>				
<b>1. Does this system contain any personal information about individuals?</b> (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.			
<b>2. Is this an electronic system?</b>	Yes			

<b>D. DATA IN THE SYSTEM</b>	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Stakeholders, public, industry, CPSC employees, and media registrants.
2. Generally describe what data/information will be collected in the system.	Name, title, affiliation, address, city, state, zip code, phone, fax, and email address.
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?	Self disclosed general information for forum registration.
4. How will data be checked for completeness?	CPSC staff will be looking at the registrant's data to determine how many people will be in attendance.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Data is supplied by registrants.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	Data elements are described in "Online Registration Form: CPSC Public Meeting: An Overview of the Consumer Product Safety Improvement Act of 2008"
<b>E. ATTRIBUTES OF THE DATA</b>	
1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?	Data is relevant and necessary for meeting registration.
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 will be used to print a list of attendee information to verify registration on the day of the meeting. Printed lists will be shredded after event.
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 will be placed in an Excel or other sheet for retrieval. It will not be in a system to search by personal identifier.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Individuals can chose not to register for meeting. There will be no use of information other than for listing the meeting's attendees.
<b>F. MAINTENANCE AND ADMINISTRATIVE CONTROLS</b>	
1. What are the retention periods of data in this system?	Information will be maintained only until meeting is concluded.
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?	There will be no reports produced on listed attendees. Hard copies of all registration information will be shredded after the meeting is concluded.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	Yes. This system will provide the capability to locate an individual name and their registration information.
4. For electronic systems only, what	There will be limited access to the information by CPSC employees. Only employees

controls will be used to prevent unauthorized monitoring?	working on and planning the event will have access to the information.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	This is not a Privacy Act System of Records.
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	Not applicable.
<b>G. ACCESS TO DATA</b>	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	IT staff, EXPA, Executive Director's staff, Chairman's staff
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	CPSC staff regularly undergoes ethics training and must adhere to principles of ethical conduct, which specify the appropriate and inappropriate use of government information by Federal employees. Hard copies of data will be shredded after conclusion of the public meeting.
3. Who is responsible for assuring proper use of the data?	The information owner and the system manager share overall responsibility for protecting the privacy rights of individuals by following established Privacy Act guidelines.
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?	No.
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?	No.