

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

Name of Project:	ATV Safety Summit
Office/Directorate:	EXHR

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	Hope Nesteruk, Engineering Psychologist, ESHF, x7694
System Owner: (Name, title, organization and ext.)	Hope Nesteruk, Engineering Psychologist, ESHF, x7694
System Manager: (Name, title, organization and ext.)	Li Wang, IT Specialist, EXIT, x7845

B. APPROVING OFFICIALS

	Signature	Approve	Disapprove	Date
System Owner	 <p>Digitally signed by HNesteruk DN: o=CPSC, ou=HQ, ou=OES, cn=HNesteruk Date: 2012.07.18 08:58:55 -04'00'</p>			
System Owner Management	 <p>Digitally signed by ROBERT OCHSMAN DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=ROBERT OCHSMAN, 0.9.2342.19200300.100.1.1#6100100002865 Date: 2012.07.18 10:16:40 -04'00'</p>			
Privacy Advocate Albert Anders, ITPP	 <p>Digitally signed by ALBERT ANDERS DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=ALBERT ANDERS, 0.9.2342.19200300.100.1.1#61001000016505 Date: 2012.07.18 11:33:20 -04'00'</p> <p>Albert Anders</p>			
Chief Information Security Officer Patrick Manley, ITTS	 <p>Digitally signed by PATRICK MANLEY DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK MANLEY, 0.9.2342.19200300.100.1.1#6100100000929 Date: 2012.07.18 14:55:46 -04'00'</p> <p>Patrick Manley</p>			
Senior Agency Official for Privacy Mary James, SAOP	 <p>Digitally signed by MARY JAMES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=MARY JAMES, 0.9.2342.19200300.100.1.1#61001000016516 Date: 2012.07.18 15:07:07 -04'00'</p> <p>Mary James</p>			
System of Record? _____Yes _____No				
Reviewing Official: Patrick D. Weddle, AED, EXIT	 <p>Digitally signed by PATRICK WEDDLE DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK WEDDLE, 0.9.2342.19200300.100.1.1#61001000044261 Date: 2012.07.19 05:16:43 -04'00'</p> <p>Patrick D. Weddle</p>			

C. SYSTEM APPLICATION/GENERAL INFORMATION

1. Does this system contain any personal information about individuals? (If there is NO information collected,	Yes
---	-----

maintained, or used that is identifiable to the individual, the remainder of PIA does not have to be completed.)	
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)	Stakeholders, public, industry, CPSC employees, and media registrants.
2. Generally describe what data/information will be collected in the system.	Name, affiliation, 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 meeting registration purposes.
4. How will data be checked for completeness?	Staff will not verify the information provided directly by the registrants.
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 prior to the meeting.
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 for ATV Safety Summit" file attached. The registration will be located on cpsc.gov during the registration period.

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?	Data is relevant and necessary for Summit registration and assist CPSC staff in selecting panelists, determining how many people will attend, limiting attendance to our facility capacity, contacting selected panelists, and for contacting attendees if the meeting is cancelled.
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 placed in an Excel spreadsheet for data retrieval. The spreadsheet will be protected using electronic access control and file system protections. 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 the 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. The data will be searchable by personal identifier, such as name, through Excel's built-in search function. There will be no use of the data other than to print the registration list to verify registration on the day of the event, notify selected panelists, and/or notify registrants in the event the Summit is canceled.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Individuals can choose not to register for a meeting, or not to provide personal information other than their name, affiliation, and email. There will be no use of information other than for listing the meeting's attendees.

F. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1. What are the retention periods of data in this system?	All hard copies of the data will be shredded after the event. The Excel file will be retained indefinitely in an access controlled file system. The Excel file will be maintained on an access controlled CPSC server indefinitely or otherwise consistent with CPSC and/or 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?	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.	The only information required is name, affiliation, and email address. If the registrant chooses to provide an address, the system will provide the capability to locate an individual; however, the data will not be used to monitor individuals in any way.

4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	There will be limited access to the information by CPSC employees. Only employees 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 currently identified as a 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
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	EXIT, ESHF, EXHR, Executive Director's staff, and the 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 uses of government information by Federal employees. Hard copies of the 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?	Yes. The registration website will be developed by a contractor and the data file created from the registration website will be maintained by a contractor. All CPSC contractors regularly undergo Privacy Act training and must adhere to principles of ethical conduct, which specify the appropriate and inappropriate uses of government information.
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?	Yes. The Excel file will be stored on a CPSC maintained server, which is remotely accessible by CPSC employees and contractors through the CPSC VPN.