





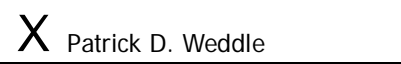
**U.S. Consumer Product Safety Commission  
PRIVACY IMPACT ASSESSMENT**

<b>Name of Project:</b>	Neighborhood Safety Network Website
<b>Office/Directorate:</b>	Office of Information and Public Affairs, OCM

**A. CONTACT INFORMATION**

<b>Person completing PIA:</b> (Name, title, organization and ext.)	Carl E. Purvis, Public Affairs Specialist, U.S. Consumer Product Safety Commission, x7805
<b>System Owner:</b> (Name, title, organization and ext.)	Office of Information and Public Affairs, U.S. Consumer Product Safety Commission X7805
<b>System Manager:</b> (Name, title, organization and ext.)	Carl E. Purvis, public affairs specialist, U.S. Consumer Product Safety Commission, x7805

**B. APPROVING OFFICIALS**

	Signature	Approve	Disapprove	Date
System Owner	 <hr/>			
Privacy Advocate Linda Glatz, ITPP	 <hr/> Linda Glatz			
Chief Information Security Officer Patrick Manley, ITTS	 <hr/> Patrick Manley			
Senior Agency Official for Privacy Mary James, SAOP	 <hr/> Mary James			
System of Record? ____ Yes <u>X</u> No				
Reviewing Official: Patrick D. Weddle, AED, EXIT	 <hr/> Patrick D. Weddle			11/14/2011

**C. SYSTEM APPLICATION/GENERAL INFORMATION**

<b>1. Does this system contain any personal information about individuals?</b> (If there is <b>NO</b> 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. This is a registration application on the CPSC website.

<b>D. DATA IN THE SYSTEM</b>	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Public, employees and contractors
2. Generally describe what data/information will be collected in the system.	First and last names, street and/or mailing addresses, e-mail addresses and telephone numbers
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 collected directly from the individual as part of a registration process.
4. How will data be checked for completeness?	Reviewed by system manager.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Periodically reviewed and updated by system manager.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	No
<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?	The data allows us to maintain a list of email addresses of subscribers to our monthly e-newsletters.
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 not being consolidated. It is password protected.
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 retrieved by an automated list-service server. The list service provides automatic mailings of safety information to those registered. Staff do not search and retrieve information by personal identifiers.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Individuals have the choice of not receiving the service.
<b>F. MAINTENANCE AND ADMINISTRATIVE CONTROLS</b>	
1. What are the retention periods of data in this system?	A record schedule has not been established yet.
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?	Names and addresses are deleted from the system at the user's request or upon determining that the e-mail address is no longer in service.
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?	Data is password protected so only authorized users have access. All authorized staff/contractors take mandatory annual Security and Privacy training and sign 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, information is not searched or retrieved by a personal identifier.

6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	NA
<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).	System administrators, contractors.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Staff/contractors with access to the system are required to take annual Security and Privacy training and sign Rules of Behavior agreements.
3. Who is responsible for assuring proper use of the data?	Office of Information and Public Affairs
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 will be required to sign non-disclosure agreements in the understanding that NSN list-serve information is confidential.
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.