U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	FOIA Tracking			
Office/Directorate:	EXIT/ITIM/OS-FOI			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Alberta E. Mills, ITIM, x7479			
System Owner: (Name, title, organization and ext.)	Alberta E. Mills, ITIM, x7479			
System Manager: (Name, title, organization and ext.)	Todd Stevenson, ITM, x6836 Alberta E. Mills, ITIM, x7479			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner	Alberta E. Mills, ITIM, x7479	✓		3/31/10
Privacy Advocate	Linda L Glatz Linda Glatz, ITPP	✓		3/31/10
Chief Information Security Officer	Patrick Manley, ITTS	✓		4/1/10
Senior Agency Official for Privacy **System of Record?** ✓ **Yes** ____ **No**	Mary James Mary Kelsey, Director, ITPP	✓		4/6/10
Reviewing Official:	Patrick D. Weddle, AED, EXIT	✓		4/6/10
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 personal information about individuals, e.g., name, home address, home telephone number, fax number, personal e-mail address and other pertinent information related to processing and responding to FOIA and Privacy Act requests.			
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)	Private citizens, attorneys, educators, health care professionals, local and state government staff.
2. **Generally describe what data/information will be collected in the system.**	Name, address, city, state, telephone number, fax and email address. Also the type of requester, such as an educational institution, media, attorney, consumer, etc.
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?**	Source of information is from the individual making the FOIA or Privacy Act request.
4. **How will data be checked for completeness?**	Data is entered based on information provided by the requester.
5. **Is the data current?** (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Recent requests will have current information; older requests may not have current information. No steps are taken to keep information up to date.
6. **Are the data elements described in detail and documented?** (If yes, what is the name and location of the document?)	The data elements are described and detailed in a document maintained by the Commission's ITTS staff.

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 system is designed to track FOIA and Privacy Act requests. The data is relevant and necessary in order for staff to provide accurate and timely responses to requests.
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.**	Access to the FOIA Tracking system is limited to CSPC FOIA staff only; staff gains access through the use of IDs and passwords.
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 is retrieved by using the FOIA request number. However, data can also be retrieved using the requester's name, company name or product code.
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?**	2 to 6 years, contingent upon the National Archives Records Administration (NARA's General 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?**	The disposition of data will adhere to the records management schedule being implemented within CPSC and/or NARA.
3. **For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**	Yes. The systems permits individuals to be identified via email or home address since these are required fields when submitting a request.
4. **For electronic systems only, what**	CPSC Network access and application User ID and password are required.

controls will be used to prevent unauthorized monitoring?	
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No, CPSC SORN is under development.
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	System is not being modified.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	CPSC FOIA staff.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Authorized staff is provided training on proper use of the data.
3. Who is responsible for assuring proper use of the data?	Director, Office of the Secretary, FOIA Officer and IT.
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.