U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	Enforcement and Investigation Files SORN CPSC-7			
Office/Directorate:	Office of General Counsel			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Pamela Brinker, Attorney, OGC, X7840			
System Owner: (Name, title, organization and ext.)	Cheryl A. Falvey, General Counsel, OGC, X7642			
System Manager: (Name, title, organization and ext.)	Not Applicable			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner	Cheryl A. Falvey, OGC	CAF		4/13/10
Privacy Advocate	Linda Glatz, ITPP	✓		4-13-10
Chief Information Security Officer	**Patrick Manley, ITTS**	✓		5/12/10
Senior Agency Official for Privacy **System of Record?** ✓ **Yes** ____ **No**	Mary James, Director, ITPP	✓		5/14/10
Reviewing Official:	Patrick D. Weddle, AED, EXIT	✓		5/17/10
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.			
2. Is this an electronic system?	The system has both electronic and paper components.			

D. DATA IN THE SYSTEM	
1. **What categories of individuals are covered in the system?** (public, employees, contractors)	All categories (public, employees, contractors). Anyone who authors, receives, or is mentioned in documents received by, or generated by, the Consumer Product Safety Commission in preparation for, or the conduct of, potential or actual administrative or judicial enforcement actions.
2. **Generally describe what data/information will be collected in the system.**	Personal information such as name of both author and addressee, as well as purely legal and technical information including memoranda, correspondence, test reports, injury reports, notes and other documents relating to the preparation for, or conduct of, potential or actual administrative or judicial enforcement actions.
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?**	The records come from individuals and organizations under investigation as well as any person, organization, or other source of information relevant to an investigation or adjudication.
4. **How will data be checked for completeness?**	Commission attorneys, compliance officers, investigators and supporting technical staff will review the materials for accuracy and completeness.
5. **Is the data current?** (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Data is continually added and updated throughout the investigation and enforcement proceedings.
6. **Are the data elements described in detail and documented?** (If yes, what is the name and location of the document?)	No.
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 is relevant and necessary to the investigation of potentially hazardous products and the enforcement of the Commission's statutory authority.
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.**	Not applicable. The data is not being consolidated.
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.**	Both paper and computer records are retrieved by name of the author or addressee or by other indicia. Additionally, computer records may be retrievable by names elsewhere in the document.
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?**	The records are kept indefinitely.
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?**	Not applicable.
3. **For electronic systems, will this system provide the capability to identify, locate, and monitor**	The system will be able to identify those persons who are, or have been, under product hazard investigation or subject to enforcement proceedings.

individuals? If yes, explain.	
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	Not applicable.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	Yes, CPSC-7
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	Not applicable. This 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).	Commission staff with a need to know and the data may be transferred to Department of Justice employees as needed for routine use under the Privacy Act for litigation in District Court or higher.
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 and privacy training and must adhere to the principles of ethical conduct which specify the appropriate and inappropriate use of government property and information by federal employees. Department of Justice employees are only provided access on a need to know for litigation purposes and are subject to all Privacy Act rules and regulations for the use of the material.
3. Who is responsible for assuring proper use of the data?	Office of General Counsel and Director of the Office of Compliance and Field Operations.
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?	The Department of Justice may gain access to the records in connection with litigation pursuant to routine use described in the Privacy Act.
7. Will any of the personally identifiable information be accessed remotely or physically removed?	The information may be accessed remotely by Department of Justice Employees or physically removed from CPSC and transferred to the Department of Justice as needed for litigation purposes. Department of Justice employees are subject to the Privacy Act requirements.