

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

Name of Project:	Concordance			
Office/Directorate:	OGC			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Abioye Ella Mosheim, Assistant General Counsel, GCOS x7545			
System Owner: (Name, title, organization and ext.)	Patricia Hanz, General Counsel, x7416			
System Manager: (Name, title, organization and ext.)	Nidhu Nijhawan, Supervisory IT Specialist, EXIT, x6812			
B. APPROVING OFFICIALS	Signature	Approv e	Disappro ve	Date
System Owner Patricia Hanz, GC	Patricia Hanz, General Counsel			
Privacy Advocate Bobby Sanderson, EXIT	Bobby Sanderson, ISSO			
Chief Information Security Officer Patrick Manley, EXIT	Patrick Manley, CISO	X X		4/30/18
Senior Agency Official for Privacy James Rolfes, EXIT				4/30/18
System of Record? _____ Yes ___X___ No	James Rolfes, CIO	X		
Reviewing Official: James Rolfes, EXIT	James Rolfes, CIO	X		4/30/18

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: personal names, emails, telephone numbers, Social Security Numbers, dates of birth, height, weight, medical reports. Some contact information is for business contacts (for large and closely-held businesses).
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)	Manufacturers' ("firms") employees; consumers who reported on or to firms; Consumer Product Safety Commission ("CPSC") employees; and anyone related to one of these groups.
2. Generally describe what data/information will be collected in the system.	Concordance is a document deduplication and management software. Firms produce documents upon CPSC's request. Those documents are used during the civil penalty phase of an investigation. The documents are loaded into Concordance for deduplication and review. Concordance is also used by CPSC in the event the agency files a complaint – CPSC will use Concordance to review agency records for privilege.
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?	Data sources include the firms; Lexis searches; third party reports; Freedom of Information Act ("FOIA") litigation. But mostly directly from firms.
4. How will data be checked for completeness?	All data in the system is reviewed by GC attorneys for completeness. Firms are also given the chance to review the data for completeness.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	The data is current at the time CPSC requests the records. If CPSC needs to update the information, it will ask for additional information. Firms are not able to self-update information.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	Yes.
E. ATTRIBUTES OF THE DATA	
1. Explain how the use of the	The data is used to support CPSC's litigation needs, including

data is both relevant and necessary to the purpose for which the system is being designed?	civil penalty investigations, and to pursue and defend against litigation.
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.	The only people with access to Concordance are CPSC OGC attorneys; the two Department of Justice (“DOJ”)-contracted litigation support technicians; and EXIT.
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.	The data will be retrieved using a firm’s name; consumer’s name; employee’s name; and key words within each case file.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Firms can reject the request for records or redact portions of records based on privileges. Firms can also decline a Section 27 subpoena. Consumers can ask to have their name and contact information withheld from the firm and the public, released to the firm, or released to the public and the firm.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	Currently all electronic data is stored 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 procedures documented?	CPSC is currently developing procedures for the disposition of electronic data. Details forthcoming.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	The system provides the capability to identify and locate individuals using names and addresses, because the records can be searched using names or addresses are keywords, but not the ability to monitor individuals.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	The system does not require a username or password but one must have pre-authorized access to the shared drive (where records are maintained) to review the records.

<p>5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?</p>	<p>No.</p>
<p>6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain</p>	<p>N/A</p>
<p>G. ACCESS TO DATA</p>	
<p>1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).</p>	<p>Authorized employees have rights to review the records. The two DOJ contractors have access to the data. EXIT also has access to the data.</p>
<p>2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)</p>	<p>CPSC provides new hires with training on the proper use of government property and security awareness training. CPSC also includes a confidential business information notice and a Section 15 notice on the Concordance records.</p>
<p>3. Who is responsible for assuring proper use of the data?</p>	<p>EXIT can segregate and protect the data, limit access to certain folders to certain employees.</p>
<p>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?</p>	<p>The Memorandum of Understanding (“MOU”) between DOJ (the agency responsible for the tech contractors) and CPSC requires a Public Trust Security Clearance. See MOU.</p>
<p>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?</p>	<p>No</p>

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?	CPSC shares the data with DOJ in the event that DOJ represents CPSC in litigation.
7. Will any of the personally identifiable information be accessed remotely or physically removed?	The data could be accessed remotely using a telework laptop, for employees authorized to telework. The data could be physically removed only by permission of EXIT to save the data onto a flash drive, CD, or other portable storage device.