


U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	General Counsel Tracking System SORN CPSC-9			
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, ITTP	✓		4-13-10
Chief Information Security Officer	Patrick Manley, ITTS			4/13/10
Senior Agency Official for Privacy	Mary James, Director, ITTP	✓		4/13/10
System of Record? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No				
Reviewing Official:	Patrick D. Weddle, AED, EXIT	✓		4/14/10
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?	Yes.			

D. DATA IN THE SYSTEM	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Employees in the Office of General Counsel
2. Generally describe what data/information will be collected in the system.	Names of employees to whom assignments are given; descriptions of assignments; start, completion and due dates; comments; names of divisions within the Office of General Counsel; and other information regarding General Counsel assignments.
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 taken from the individual as well as other employees and clients.
4. How will data be checked for completeness?	The assigning supervisor will conduct a completeness review once the assignment is completed.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Supervisors and administrative employees routinely update and input data.
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 ensuring that legal assignments are timely completed and queries from other units of CPSC are addressed and to assist in the evaluation of the attorneys' performance based on the types of assignments performed and timeliness of completion.
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.	The data can be retrieved by any field, including attorney name. Reports can be created regarding an individual's past and current assignments based on the employee's name; subject matter of the assignment; assigned, completed and due dates; or name of a division within the Office of General Counsel.
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?	No set retention length.
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?	Old records are destroyed based on a need for computer storage space.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	Yes, this system will allow supervisors to monitor the workload and types of assignments completed by an individual within the Office of General Counsel.
4. For electronic systems only, what	The system is password protected and can only be accessed by Office of General

controls will be used to prevent unauthorized monitoring?	Counsel supervisory and administrative staff.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	Yes, CPSC-9
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).	Office of General Counsel supervisory and administrative staff.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	The Office of General Counsel 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. Additionally, only supervisory and administrative staff may create records, assign or extend due dates, or enter completion dates.
3. Who is responsible for assuring proper use of the data?	Office of General Counsel.
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.