U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	Disability Accommodation Files			
Office/Directorate:	Office of Equal Employment Opportunity			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Tamatha Brigham, Office Manager, x7501			
System Owner: (Name, title, organization and ext.)	Office of Equal Employment Opportunity			
System Manager: (Name, title, organization and ext.)	Kathleen Buttrey, Director, Office of Equal Employment Opportunity			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner Kathleen Buttrey, EEO	11/1/2011 X Kathleen Buttrey			
Privacy Advocate Linda Glatz, ITPP	11/1/2011 X Linda Glatz Linda Glatz			
Chief Information Security Officer Patrick Manley, ITTS	11/10/2011 X Patrick Manley Patrick Manley			
Senior Agency Official for Privacy Mary James, SAOP **System of Record? (CPSC-23)** __x__Yes _____No	12/1/2011 X Mary James Mary James			
Reviewing Official: Patrick D. Weddle, AED, EXIT	X PATRICK WEDDLE Digitally signed by PATRICK WEDDLE DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK WEDDLE, 0.9.2342.19200300.100.1.1=61001000044261 Date: 2011.12.02 06:57:08 -05'00' Pactrick D. Weddle			
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, records are kept both electronically and in paper form.			

D. DATA IN THE SYSTEM	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Employees.
2. Generally describe what data/information will be collected in the system.	Name, title, address, date of birth, sex, race, national origin and medical information.
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 obtained directly from individual.
4. How will data be checked for completeness?	Data is verified by or with employee and EEO specialist.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Data is kept current with regular contact with employee.
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 information is gathered for reasonable accommodation purposes and for tracking.
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 files are stored on a network drive or on Sharepoint and anyone needing access will be granted access to the file over the network.
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 employee name or tracking number.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Employees can decline to provide the information, however they will not get an accommodation.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	Three years from date of last action.
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?	Data is shredded at the end of retention period.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No, the system will not provide the capability to identify and monitor individuals.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	Data is maintained on hard drive only in an agency-secured system. Only staff with "need to know" will have access to the data. The data is password protected. The data is primarily in email and word documents. If access is required by offices other than EEO, the file would be made available through access to the network drive or Sharepoint file.
5. Is this system currently identified as a CPSC system of records? If so,	Yes. CPSC-23

under which notice does the system operate?	
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	The system is not being modified at this time. Future changes to the system could result in changes to the Privacy Act system of records.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	EEO Director and EEO specialists in the Office of Equal Employment Opportunity.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Paper information is maintained in locked file cabinets in secure office space. Electronic information is stored in CPSC secured computer system and is password protected.
3. Who is responsible for assuring proper use of the data?	Director, Office of Equal Employment Opportunity.
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.