U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT

Name of Application/System:	
Office/Directorate:	
Date:	

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	
System Owner: (Name, title, organization and ext.)	
System Manager/Technical POC: (Name, title, organization and ext.)	

B. APPROVING OFFICIALS

System Owner	Date
Privacy Officer	Date
Chief Information Security Officer (CISO)	Date
Asst. General Counsel for FOIA, Records and Privacy	Date
Senior Agency Official for Privacy (SAOP)	Date

C. SYSTEM OF RECORDS NOTICE

1. Will the system or application maintain records that contain information about individuals?   Yes ❑   No ❑

2. Will the system or application allow records to be retrieved by a personal identifier*?   Yes ❑   No ❑

If the answer to both 1 and 2 above is "Yes," then the system requires a System of Records Notice (SORN).

* *A personal identifier might include an individual's name, address, email address, telephone number, social security number, photograph, biometric information, or any other unique identifier that can be linked to an individual.*

D. PRIVACY ASSESSMENT

1. Will the system or application be used to collect, store, or transmit personally identifiable information (PII)*?

Yes ❑   No ❑   (If there is **NO** information collected, stored, or transmitted that is identifiable to the individual, the remainder of this PIA does not have to be completed.)

* Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. (e.g. Social Security numbers, Passport numbers, etc.)	
2. Generally describe the type of information that will be collected, stored, or transmitted.	
3. What categories of individuals are covered in the system? (public, employees, contractors)	

E. SYSTEM DATA

4. Is the PII collected verified for accuracy? Why or why not?	
5. Is the PII current? How is this determined?	
6. Who will be responsible for protecting the privacy of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability?	
7. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	
8. 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?	

F. MAINTENANCE AND ADMINISTRATIVE CONTROLS

9. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	
10. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII.	
11. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?	
12. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?	
13. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)?	
14. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	

G. ACCESS TO DATA

15. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	

16. What controls are in place to prevent unauthorized access to the data?	
17. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access?	
18. Is access to the PII being monitored, tracked, or recorded?	
19. For CPSC support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval?	
20. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared?	
21. What CPSC personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)?	
22. Will any of the personally identifiable information be accessed remotely or physically removed?	