

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

Name of Project:	Lab Information Management System
Office/Directorate:	EXIT

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	Brett Layton, IT Project Manager, EXIT, 7488
System Owner: (Name, title, organization and ext.)	Andrew Stadnik, Associate Executive Director for Laboratory Sciences, LS, 301-987-2037
System Manager: (Name, title, organization and ext.)	John Gilmore, Data Acquisition, IT and Calibration Systems Specialist, LS, 301-987-2309

B. APPROVING OFFICIALS	Signature	Approve	Disapprove	Date
-------------------------------	------------------	----------------	-------------------	-------------

System Owner	Andrew Stadnik, Associate Executive Director for Laboratory Sciences	X		9/20/16
Privacy Advocate Bobby Sanderson, EXIT	Bobby Sanderson, ISSO	X		
Chief Information Security Officer Patrick Manley, EXIT	Patrick Manley, CISO	✓		
Senior Agency Official for Privacy Mary James, EXIT System of Record? ____ Yes <u> X </u> No	Mary James, Deputy CIO J. Rolfes for Mary James	X		9/26/2016
Reviewing Official: James Rolfes, EXIT	James Rolfes, CIO	X		9/26/2016

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.)	No
2. Is this an electronic system?	

D. DATA IN THE SYSTEM

1. What categories of individuals are	
--	--

covered in the system? (public, employees, contractors)	
2. Generally describe what data/information will be collected in the system.	
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?	
4. How will data be checked for completeness?	
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	
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?	
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.	
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.	
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	
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?	
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	

4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	
5. Is this system currently identified as a CPSC system of records? If so, 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	
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	
3. Who is responsible for assuring proper use of the data?	
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?	
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?	
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?	
7. Will any of the personally identifiable information be accessed remotely or physically removed?	