



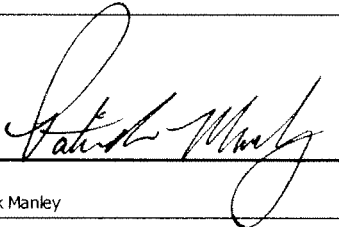

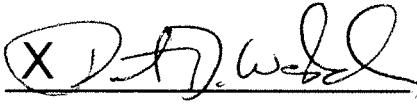
**U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT**

Name of Project:	Respirator Program Medical Reports
Office/Directorate:	EXIT

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	Ron Welch, Administrative Services Specialist, TSFS x7091
System Owner: (Name, title, organization and ext.)	Ron Welch, Administrative Services Specialist, TSFS, x7091
System Manager: (Name, title, organization and ext.)	Ron Welch, Administrative Services Specialist, TSFS, x7091

B. APPROVING OFFICIALS

	Signature	Approve	Disapprove	Date
System Owner	12/20/2011 <u>X  Ronald P. Welch</u> 12/20/11	✓		12/20/11
Privacy Advocate Linda Glatz, ITTP	12/20/2011 <u>X Linda Glatz </u> Linda Glatz	✓		12/21/11
Chief Information Security Officer Patrick Manley, ITTS	<u>X </u> Patrick Manley	✓		12/21/11
Senior Agency Official for Privacy Mary James, Director, ITTP	<u>X </u> Mary James	✓		12/21/11
System of Record? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No				
Reviewing Official: Patrick D. Weddle, AED, EXIT	<u>X </u> Patrick D. Weddle	✓		12/21/11

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. Name, date of birth, social security number and respirator test findings. Social Security numbers have been eliminated on the reports, however, older files still contain the numbers.
2. Is this an electronic system?	No.

D. DATA IN THE SYSTEM	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Employees and contractors whose jobs may require them to wear respirators.
2. Generally describe what data/information will be collected in the system.	Medical reports indicating (a) approval or disapproval for an employee's use of respirators, (b) allowable level of exertion and any medical conditions relevant to the use of respirators; and (c) recommended interval until next medical evaluation.
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?	The information contained in the reports are prepared by Federal Occupation Health, HHS.
4. How will data be checked for completeness?	CPSC does not check 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?)	Data is required to be updated annually.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	Data is collected by HHS, Federal Occupational Health office. CPSC does not have documentation of their process.
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?	These reports are used to keep track of employees who are authorized to work in hazardous environments requiring the use of respirators and to schedule repeat medical examinations for those employees.
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.	N/A – not an electronic system.
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.	Hard copy records are retrieved by name of employee.
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?	There is no established NARA record schedule. Until a record schedule is established, records are maintained 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 the procedures documented?	Records are maintained indefinitely.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	Records are retrieved by name of employee.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	NA
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	SORN CPSC-24

6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	No, 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).	System administrator and subject employee have access to the data.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Records are kept in a combination lock safe type filing cabinet. Only system administrator has access to records.
3. Who is responsible for assuring proper use of the data?	System administrator.
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, contractors are not involved with the design, development, or maintenance of the system.
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 other systems share data or have access to the data.
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.