U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	Key Fob/Access Card Control Devices			
Office/Directorate:	EXIT/ITTS			
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.)	DataWatch Systems, Inc.			
System Manager: (Name, title, organization and ext.)	Ron Welch, Administrative Services Specialist, TSFS, x7091			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner	X Ronald P. Welch			12/28/11
Privacy Advocate Linda Glatz, ITPP	X Linda L Glatz Linda Glatz	✓		12/21/11
Chief Information Security Officer Patrick Manley, ITTS	X Patrick Manley Patrick Manley	✓		12/21/11
Senior Agency Official for Privacy Mary James, SAOP **System of Record?** ____Yes _X_ No	X Mary James Mary James	✓		12/28/11
Reviewing Official: Patrick D. Weddle, AED, EXIT	X P D. Wedd Pactrick D. Weddle	✓		12/28/11
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.)	No. These are access control devices that allow entry to CPSC spaces; only employee name is associated with the access card/fob. No other personal information is used.			
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, contractors, and others who have received uniquely coded key fobs to gain access to various parts of Commission facilities.
2. Generally describe what data/information will be collected in the system.	Reports which show the time fob has been used; the identity of the fob and, therefore, of the person to whom it is assigned; the location at which it has been used; and the access privileges of the person to whom it is assigned.
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?	Source of information is from fob in possession of employee/contractor.
4. How will data be checked for completeness?	Employee/contractor employment is verified at time of fob assignment.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	TSFS is notified by Personnel Office when employee or contractor is terminated so that fob can be collected or deactivated. This is part of the checkout procedure.
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 necessary to maintain the security of government space and may be used to investigate breaches of security, theft, vandalism, other property losses, criminal offenses, and employee misconduct.
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.	Only two CPSC System Administrators have access to the DataWatch system. Access to the data is password protected.
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 can be retrieved by fob/card number, employee name, or time and dates.
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?	Data is retained for eight months after an employee/contractor leaves the agency or is no longer assigned a fob. There is no current NARA schedule for these records.
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?	The records are kept for eight months from the date of creation and then destroyed.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	This system will provide the capability to monitor employee/contractor building entry and exit for the purposes of an OIG investigation or law enforcement. Senior management must authorize the investigative requests before data is obtained.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	Only authorized staff have access to the system which is password protected.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	Yes, CPSC-11

6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	System is not being modified at this time.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	CPSC Contractor and two CPSC system administrators.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	These records are kept in a secure computer facility and can be retrieved only by the Commission's Physical Security Manager or designee upon request of a senior Commission official or a law enforcement officer. Printouts are stored in locked file cabinets in secure locations. The system administrators have completed annual Security and Privacy training.
3. Who is responsible for assuring proper use of the data?	System administrators
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?	Contractors design, collect data, produce reports upon request, and monitor the system. The only personal information in the system is the name of the employee.
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?	Data is not shared with other agencies.
7. Will any of the personally identifiable information be accessed remotely or physically removed?	No.