U.S. Consumer Product Safety Commission **PRIVACY IMPACT ASSESSMENT**				
Name of Project:	Data Loss Prevention System			
Office/Directorate:	EXIT			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Denis Suski, Chief – TSNE x6724			
System Owner: (Name, title, organization and ext.)	Denis Suski, Chief – TSNE x6724			
System Manager: (Name, title, organization and ext.)	Denis Suski, Chief – TSNE x6724			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner	Denis Suski, TSNE			5/19/09
Privacy Advocate	Linda Glatz, ITPP	LG		5-19-09
Chief Information Security Officer	Patrick Manley, ITTS			5/20/09
Senior Agency Official for Privacy **System of Record?** ____**Yes** [✓ **No**]	Mary Kelsey Mary Kelsey, Director, ITPP			5/20/09
Reviewing Official:	Acting for Patrick D. Weddle, AED, EXIT			6/2/09
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			

D. DATA IN THE SYSTEM	
1. **What categories of individuals are covered in the system?** (public, employees, contractors)	Public, employees, contractors
2. **Generally describe what data/information will be collected in the system.**	Data may contain name, address, telephone number, social security number, email address, date of birth or other personally identifiable 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?**	In some cases information comes directly from individual such in cases of project injury information submitted directly to CPSC. Other information may come from personnel and financial records systems maintained by CPSC.
4. **How will data be checked for completeness?**	Data is pulled from existing data systems and will not 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 **Is the data current?** (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Data is pulled from existing data systems
6. **Are the data elements described in detail and documented?** (If yes, what is the name and location of the document?)	There is no documentation for this data loss prevention system. Individual data bases that will be monitored may have documentation.
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?**	System is designed to detect possible data system breaches as they relate to data security for personal information
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 EXIT data administrators and contractor providing software will have access to the 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.**	There are no plans to retrieve information by individual personal identifiers
4. **What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?**	There is no new information obtained for this data loss prevention system. It will monitor data in existing systems.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. **What are the retention periods of data in this system?**	Data will be retained until detection system can be evaluated for possible future acquisition
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 will be wiped from servers once evaluation is complete
3. **For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**	No
4. **For electronic systems only, what**	Password protected

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?	No
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	Not applicable

G. ACCESS TO DATA

1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	Contractors and data administrators in EXIT will 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.)	System is password protected. Staff and contractors have completed Privacy Training.
3. Who is responsible for assuring proper use of the data?	Denis Suski
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?	The contractor (Symantec Corp.) will be involved in the design of the system for the Proof of Concept. The contractor will not be involved in the maintenance of the system. The contractor will not have access to the data collected by 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
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.