U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	IFS			
Office/Directorate:	EXC			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Scott Simmons, Director of Resources Management, Office of Compliance and Field Operations, EXC, 7574			
System Owner: (Name, title, organization and ext.)	Carol Cave, Deputy Director, EXC, x7677			
System Manager: (Name, title, organization and ext.)	Nidhu Nijhawan, Supervisory IT Specialist, EXIT, x6812			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner Carol Cave, Deputy Director	CAROL CAVE Digitally signed by CAROL CAVE DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=CAROL CAVE, 0.9.2342.19200300.100.1.1=61001000029846 Date: 2018.04.26 12:15:17 -04'00' Carol Cave, Deputy Director	☐	☐	
Privacy Advocate Bobby Sanderson, EXIT	YOUSSEF TAKHSSAITI Digitally signed by YOUSSEF TAKHSSAITI DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=YOUSSEF TAKHSSAITI, 0.9.2342.19200300.100.1.1=61001003095079 Date: 2018.05.01 10:41:43 -04'00' Bobby Sanderson, ISSO	☐	☐	
Chief Information Security Officer Patrick Manley, EXIT	PATRICK MANLEY Digitally signed by PATRICK MANLEY DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK MANLEY, 0.9.2342.19200300.100.1.1=61001000000929 Date: 2018.04.26 14:50:00 -04'00' Patrick Manley, CISO	X☐	☐	4/26/18
Senior Agency Official for Privacy James Rolfes, EXIT **System of Record?** _____**Yes** _X__**No**	JAMES ROLFES Digitally signed by JAMES ROLFES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=JAMES ROLFES, 0.9.2342.19200300.100.1.1=61001001116382 Date: 2018.04.30 17:41:01 -04'00' James Rolfes, CIO	X☐	☐	4/30/18
Reviewing Official: James Rolfes, EXIT	JAMES ROLFES Digitally signed by JAMES ROLFES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=JAMES ROLFES, 0.9.2342.19200300.100.1.1=61001001116382 Date: 2018.04.30 17:41:28 -04'00' James Rolfes, CIO	X☐	☐	4/30/18
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
2. Generally describe what data/information will be collected in the system.	Firm information, product information, contact information, and consumer 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?	Some information is received directly from individuals, sometimes the information comes from import documents, other times the information comes from Lexus-Nexus
4. How will data be checked for completeness?	Compliance Officer, Field Inspector ,Clearinghouse, the data is also audited on a periodic basis
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	Yes, and it goes back to 1996
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	There are 3 tables that contain PII. Sample, Comply and Assignment tables
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 stored provides information about companies that violate CPSC mandatory requirements as well as product information to alert staff to emerging hazards. It further provides the foundation for the Office of Import Surveillance to develop and improve their targeting systems.
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.	Access to the data is restricted
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.	The data can be retrieved by company name or sample number, but not by individuals name. You can pull data by Compliance Officer (no PII), sample number, or company listed (firm), and only by a CPSC employee with access to IFS.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	The agency requests consent of disclosure of information from consumers during an investigation, individuals have the opportunity to say no, specifically on whether their contact information can be shared.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	From date of creation of the record until the end of time
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?	There is no end date, system records remain indefinite. However, paper files/records associated with IFS case data are archived. The Protection of Personally Identifiable Information for CPSC Information Systems, Directive 0760.2.
3. For electronic systems, will this system provide the capability to	The system will provide the address of the company

identify, locate, and monitor individuals? If yes, explain.	
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	Two factor authentication, in addition to access to IFS.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No, To be considered a system of records within the meaning of the Privacy Act, records that OPM maintains must be retrieved by a person's name or other personal identifying information (referred to as a "personal identifier"). 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. This means the requirements mandated by the Privacy Act are not applicable to OPM records unless the records are retrieved by a personal identifier. Mere maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to trigger the conduct of a privacy impact assessment (PIA). Yes, CPSC-8
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	N/A, because this system is not a SOR. No. Most recent SORN applies to current system scope and functions.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	Contractors, Managers, Compliance Officers and Analysts
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Permission specifications, training, IFS handbook, system help feature
3. Who is responsible for assuring proper use of the data?	Managers and individuals accessing 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?	Yes, contractors were involved in the development of the system and are involved with the maintenance. Yes, the Privacy Act contract clause is inserted into the contract.
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?	Yes, the DCM system communicates with IFS on recalls and sample tracking. EXC management and staff
6. Will other agencies share data or have access to the data in this	No

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?	Yes, employees may take a hard copy of a case file to work on at home or at a telework site.