United States
Consumer Product Safety Commission

Privacy Threat Analysis (PTA)/Privacy Impact Assessment (PIA)	
Name of Application/System:	International Trade Data System/Risk Assessment Methodology (ITDS/RAM)
Office/Directorate of System Owners:	Office of Information and Technology Services (EXIT)
Office/Directorate of Business Owners:	Office of Import Surveillance (EXIS)
Date:	April 20, 2023
A. Contact Information	
Person Completing PTA/PIA: (Name, title, organization)	Dennis Wallick, Contractor, EXIT
System Owner: (Name, title, organization)	Padma Chari, Information Technology Solutions Development (ITSD) Division Director, EXIT
System Manager/Technical POC: (Name, title, organization)	Brett Layton, Program Manager, EXIT
B. Approving Officials	
PADMA CHARI	Digitally signed by PADMA CHARI Date: 2023.08.14 08:15:34 -04'00'
System Owner	
CAITLYN BORGHI	Digitally signed by CAITLYN BORGHI Date: 2023.08.09 11:38:24 -04'00'
Chief Privacy Officer (CPO)	
KHALID NUMAN AL-HASSAN	Digitally signed by KHALID NUMAN AL-HASSAN Date: 2023.08.10 15:19:46 -04'00'
Chief Information Security Officer (CISO)	
ABIOYE OYEWOLE	Digitally signed by ABIOYE OYEWOLE Date: 2023.08.31 10:41:52 -04'00'
Assistant General Counsel for Freedom of Information Act (FOIA), Records, and Privacy	
JAMES SMITH	Digitally signed by JAMES SMITH Date: 2023.09.01 08:06:49 -04'00'
Senior Agency Official for Privacy (SAOP)	

C. System of Records Notice	
1. Will the system or application maintain records that contain information about individuals? (Yes or No)	Yes
2. Will the system or application allow records to be retrieved by an individual's name or by some identifying number, symbol, or other identifier assigned to the individual? (Yes or No)	Yes
3. Will the records maintained by the system or application be considered a new collection of records? (Yes or No)	Yes
If the answers to Questions 1 and 2 are yes and you do not currently have a System of Records Notice (SORN), one will be required.	
D. Privacy Threshold Analysis (PTA)	
4. Will the information system or application be used to collect, store, or transmit personally identifiable information (PII)? (Yes or No)	Yes
5. Has a Privacy Impact Assessment (PIA) ever been performed for the information system or application? (Yes or No)	Yes
6. Is there a Privacy Act System of Records Notice (SORN) for this information system or application? (Yes or No)	Yes
If any of the answers to Questions 4 through 6 are "Yes" then complete the Privacy Impact Assessment (PIA) section (F) of this document. If the answers to Questions 4 through 6 are all "No" then a PIA is not needed. Complete section E below, sign form, and return to the Chief Privacy Officer.	
E. Omission of a Privacy Impact Assessment	
7. Briefly describe the information system or application and provide a supporting statement that explains why a PIA is not needed.	N/A
F. Privacy Impact Assessment (PIA)	

8. Generally describe the type of information that will be collected, stored, or transmitted.	The types of personally identifiable information (PII) collected and stored in ITDS/RAM are names, Social Security numbers (SSNs), addresses, Consignee IDs and other items relevant to imported goods. The system collects and stores Importer IDs which could be individuals' SSNs. Under the Improvement Act of 2008, also known as the Consumer Product Safety Act (CPSIA), we were tasked by Congress to develop the International Trade Data System (ITDS)/Risk Assessment Methodology (RAM) under Section 222 of the law. CPSC uses the information to identify shipments of consumer products that are of higher risk to be able to examine them at the port. Our staff collocate and coordinate directly with Customs and Border Protection (CBP) Officers to conduct these exams. The Office of Import Surveillance (EXIS) is the primary office to use the system. Compliance Field Investigation (CFI) also uses it to provide exam information directly into the system. CFI supervisors are also able to search and target entry information similar to EXIS port staff. Data that is produced in the system is transferred into the Integrated Field System (IFS) for case management and associated downstream processes (case and legal functions). EXIS and CFI are the only offices that directly access ITDS/RAM. EXIS routinely shares information with CBP. EXIS/CFI can also share information with Office of Compliance and Field Operations (EXC) and to a lesser degree, the Office of General Counsel (OGC). Once a case is developed, CPSC may ask CBP if data can be shared with the Department of Justice (DOJ) for case work. Other functions, including reporting performance, may involve other Executive Offices. Routine data sharing is done within secure systems and normally not encrypted. Data shared with other agencies will be encrypted, per EXIS policies and procedures.
9. What categories of individuals are covered in the system? (For example, public, employees, contractors)	The category of individuals covered in the system are public businesses. These tend to be consumer direct to consumer (D2C), private businesses that range from large multinational concerns to sole proprietorships and non-profit entities. They are identified as domestic (using Taxpayer Identification Numbers (TINs) or SSNs) or foreign (using a Foreign Importer number).

10. Is the personally identifiable information (PII) collected verified for accuracy? Why or why not?	CPSC does not verify the PII collected for accuracy. Data is provided by the importer and submitted to CBP. CBP forwards the data to CPSC. CBP is responsible for the accuracy of the information it provides to CPSC. Misclassification and misrepresentation are violations of law punishable by fines and penalties against import bonds. CBP does what they can to assure this data is as accurate as necessary for their purposes.
11. Is the PII current? How is this determined?	Data is provided by the importer and currency is determined by CBP.
12. Who will be responsible for protecting the privacy of the individuals whose PII is collected, maintained, or shared in the system? Have policies and/or procedures been established for this responsibility and accountability?	The Chief Information Officer in the Office of Information and Technology Services and the Director of the Office of Import Surveillance are responsible for protecting the privacy of the individuals whose PII is collected, maintained, and shared in the system. EXIS has policies and procedures for handling how system information is shared when the system is accessed. The policies and procedures also cover the sharing of information taken from the system. The system is designed to ensure the security of PII by limiting access to only authorized users. User access is granted on an as-needed basis by EXIT and EXIS, with EXIS approving users outside of EXIS. Dual factor authentication is utilized to protect against unauthorized system access.
13. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	Yes, there is a process for individuals to have inaccurate PII corrected or amended. Individuals can resubmit incorrect data to CBP. CBP then forwards changes to CPSC.
14. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?	CPSC receives information from CBP. The broker, a business entity who represents the importer, collects the information as a routine process of entry filing. They submit to CBP through the Automated Commercial System (ACE) as required by law. Then CBP sends information to CPSC as jurisdiction allows, per the Harmonized Tariff Code declared by the importer on entry. The Automated Commercial Environment (ACE) is the primary system for processing trade-related import and export data required by government agencies. The ACE Secure Data Portal (ACE Portal) is a web-based entry point for ACE. It provides a centralized, online access point to connect CBP, trade representatives, and government agencies involved in importing and exporting goods into and out of the United States.

15. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	U.S. law requires importers to provide CBP information that contains PII in conjunction with commercial entry documents submission that support importing commodities or merchandise into or through the United States. Importer identity, manufacturer or supplier, and other parties involved in the import transaction and supply chain are necessary for commercial entry acceptance. Failure to provide required information will result in rejection of the commercial entity and the issuance of an order by CBP to remove the commodity form the territory of the United States. When importers submit the required information to ACE, they fulfill their legal requirements and they consent to how CBP will use their data. Brokers have the opportunity to correct the entry record through the entry review process with CBP.
16. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII.	Yes, other systems that interconnect to ITDS/RAM share, transmit, or access PII from the system. 1. CPSC Data Lake – CPSC Data Lake is a central repository for all CPSC data. All the ITDS/RAM core tables, including PII, goes into the Data Lake. Access to ITDS/RAM data within the Data Lake is approved and assigned by the EXIS data owner. 2. IFS – Exams that are performed at the ports that result from CBP data review will have same information directly fed to the IFS to provide the most accurate and relevant information to be able to perform essential compliance activities, such as filing Notice of Violations (NOVs) on violative products. PII is necessary in IFS from ITDS/RAM to be able to coordinate with the concerned parties. 3. ACE – ACE connects via an upstream feed to ITDS/RAM. This allows CPSC to target and coordinate on exams with CBP.
17. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?	Contractors are responsible for development and operation of the system. Recent system modifications have reduced the propensity for PII to be shared with other offices. For example, PII is masked within the Data Lake. Clauses in the relevant contract state that the contractor and its employees will not disclose any data obtained or developed under the contract to third parties without the consent of the CPSC contracting officer and that the contractor will obtain a non-disclosure agreement for each employee who will work on this contract and have access to data obtained or developed under this contract.

18. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?	Records with PII are currently retained indefinitely pending schedule approval by the National Archives and Records Administration.
19. What are the procedures for disposition of PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed? (For example, shredding, degaussing, overwriting)	Records without PII are not currently retained in the system. Records without PII are overwritten and deleted every two years. There are investigative reports and artifacts that use this data that will be part of the record in cases and compliance actions.
20. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	This system is currently identified as a CPSC system of records: CPSC-33, May 15, 2012. [FR Doc 2012-12060]
21. Who will have access to the data in the system? (For example, contractors, managers, system administrators, developers, other)	EXIS management and field investigators; contractors for the system; EXIT management, security and network specialists; and designated CFI supervisors will have access to the data in the system.
22. What controls are in place to prevent unauthorized access to the data?	The system is designated as not available for public release. All user access is controlled and managed by the Director, Office of Import Surveillance, in conjunction with EXIT staff. EXIS staff review access for the following program offices: EXIS and EXC. EXIT manages access for development staff. CPSC has designated this system a medium security system, as it is used for Law Enforcement purposes. As an LEO system, the Commission must make appropriate safeguards and separate/segregate the data properly.
23. What controls are in place to prevent the	Application logins are logged and invalid login attempts are recorded and reported.

misuse of PII by those having access?	
24. Is access to the PII being monitored, tracked, or recorded?	Yes, access to the PII is being tracked and recorded. Application logins are logged. Data tables containing PII have a record of changes.
25. For CPSC support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval?	Access to PII is determined by job responsibility, which fall into two categories: inspection by Compliance investigators and data analytics by EXIS management.
26. What third-party organizations will have access to the PII? Who establishes criteria for what PII can be shared?	No third-party organizations will have access to the PII.
27. What CPSC personnel roles will have access to PII fields? (For example, users, managers, system administrators, developers, contractors, other)	EXIS management and field investigators; EXIT management, security and network specialists; and cleared contractors will have access to PII fields in ITDS/RAM.
28. Will any of the PII be accessed remotely or physically removed?	Access to the system will be through the CPSC network only from within the firewall, or remotely via VPN through the CPSC firewall. This is a secure connection and is approved by EXIT management. Data transfer from CBP to CPSC is secured and encrypted in accordance with Inter-Agency Security Agreements.