United States
Consumer Product Safety Commission

Privacy Threat Analysis (PTA)/Privacy Impact Assessment (PIA)	
Name of Application/System:	Case Management System (CMS)
Office/Directorate of System Owners:	Office of Compliance and Field Operations (EXC)
Office/Directorate of Business Owners:	EXC
Date:	11/20/2023
A. Contact Information	
Person Completing PTA/PIA: (Name, title, organization)	Shaun Keller, Division Director, CRE
System Owner: (Name, title, organization)	Jennifer Sultan, Deputy Director, EXC
System Manager/Technical POC: (Name, title, organization)	Padma Chari, Director of Solutions Development, Office of Information and Technology Services (EXIT)
B. Approving Officials	

Jennifer Sultan
Digitally signed by Jennifer Sultan
Date: 2024.05.03 13:18:07 -04'00'

System Owner

CAITLYN BORGHI
Digitally signed by CAITLYN BORGHI
Date: 2024.05.03 12:32:44 -04'00'

Chief Privacy Officer (CPO)

KHALID NUMAN AL-HASSAN
Digitally signed by KHALID NUMAN AL-HASSAN
Date: 2024.05.03 15:40:48 -04'00'

Chief Information Security Officer (CISO)

ABIOYE MOSHEIM OYEWOLE
Digitally signed by ABIOYE MOSHEIM OYEWOLE
Date: 2024.05.03 12:35:07 -04'00'

Assistant General Counsel for Freedom of Information Act (FOIA), Records, and Privacy

Digitally signed by BRYAN BURNETT
DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=BRYAN BURNETT, 0.9.2342.19200300.100.1.1=61001000009719
Date: 2024.05.30 22:35:19 -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, but the normal retrieval method is by using a randomly generated unique identifier number.
3. Will the records maintained by the system or application be considered a new collection of records? (Yes or No)	No
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)	No
6. Is there a Privacy Act System of Records Notice (SORN) for this information system or application? (Yes or No)	No
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.	Authority to collect identification information is under 15 U.S.C. § 2065(c). This information is used to notify firms and individuals of inspection outcomes, product testing determinations, and notification of requested corrective actions. The types of information processed in the CMS include firm information (name, address, phone number), product identification (name, brand, model, style), contact information (person of contact and title, email address and phone number), and consumer information (purchasers of a product, involved in an incident, next of kin of death).
9. What categories of individuals are covered in the system? (For example, public, employees, contractors)	The individuals covered in this system are members of the public and CPSC employees.
10. Is the personally identifiable information (PII) collected verified for accuracy? Why or why not?	The information collected is not verified for accuracy, but the information is often received directly from individuals or comes from official import documents. Online seller information is often obtained from the third-party platform.
11. Is the PII current? How is this determined?	Yes, the PII is current. It comes from samples collected starting 10/1/2023 and cases created in the new system as of 11/1/2023.
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?	Individual Compliance Officers, Compliance Investigators, and analysts will all be responsible for protecting the privacy of the individuals whose PII is collected, maintained, or shared in the system. Permission specifications and training on how to use CMS and protect the information it stores, and system help features will be established.
13. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	Yes, inaccurate PII may be corrected or amended by the Compliance Officers and Compliance Investigators when identified.

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?	Yes, the source of the information is often the individual which maybe during an establishment inspection or at time of sample collection. Other sources include from other government agencies at time of importation. This information is then transcribed into the Sample Collection reports within the CPSC Integrated Field System (IFS). Finally, individuals will include PII when reporting under section 15(b) of the Consumer Product Safety Act from the relevant firms.
15. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	When information is provided at the port of entry by an importer, the importer may choose to decline to provide information if they no longer wish to import their product. Firms reporting under section 15(b) of the Consumer Product Safety Act are required to provide information
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, the CMS will connect to IFS and the CPSC Data Lake. CMS is not a complete system yet, so IFS is still utilized to initiate a case (e.g., assignments which documents investigations) and document the product that was collected for further evaluation (e.g., Sample Collection Data). Data collected across multiple systems are stored in CPSC Data Lake for the purpose of analysis, targeting, and data preservation.
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?	CPSC has engaged contractors to design, test, and deploy the CMS. The Statement of Work for the contract specifies that the contractor and its employees will not disclose any data obtained or developed under the contract without the consent of the CPSC Contracting Officer Representative. The contractor must also obtain an NDA from each employee who will work on the contract or have access to data obtained or developed under the contract.
18. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who	The underlying records are covered by CPSC's official National Archives and Records Administration approved records schedule NI-424-92-1, item 2, and must be retained onsite for one year after closure of the file, then destroyed after 15 years.

establishes the retention guidelines?	
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)	There is currently no electronic records management system in place for CMS. Compliance is working with CPSC's Information Technology Services program office to create and implement an ERM that will comply with the underlying records schedule associated with the PII.
20. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No.
21. Who will have access to the data in the system? (For example, contractors, managers, system administrators, developers, other)	Individual Compliance Officers, Compliance Investigators, analysts, managers, and Data Lake users with permission will have access to the data in the CMS.
22. What controls are in place to prevent unauthorized access to the data?	Only internal CPSC users will have access to the CMS. To sign in, users must authenticate with their Personal Identity Verification (PIV) cards. Logging is enabled and logs are retained for monitoring.
23. What controls are in place to prevent the misuse of PII by those having access?	CPSC employees and contractors are required to take annual privacy training and sign a Rules of Behavior agreement documenting their responsibilities in protecting PII. Logging is enabled in the CMS and logs are retained for monitoring.
24. Is access to the PII being monitored, tracked, or recorded?	Users' actions will be recorded in CMS and transferred to Splunk, EXIT's security analysis tool, for review.
25. For CPSC support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities	Access to the PII in CMS is granted by EXC only for employees or contractors who need access to perform their job function or are reviewing a case for legal or compliance reasons.

regarding access documented? Does access to PII require manager approval?	
26. What third-party organizations will have access to the PII? Who establishes criteria for what PII can be shared?	Contractors for the Office of Import Surveillance (EXIS) have access to CMS data via the Data Lake. Only certain users are granted access to CMS data in the Data Lake. EXIS contractors use this data to target incoming shipments.
27. What CPSC personnel roles will have access to PII fields? (For example, users, managers, system administrators, developers, contractors, other)	Individual Compliance Officers, Compliance Investigators, analysts, managers, contractors, and Data Lake users with permission will have access to PII fields in the CMS.
28. Will any of the PII 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.