U.S. Consumer Product Safety Commission PRIVACY THREAT ANALYSIS/PRIVACY IMPACT ASSESSMENT	
Name of Application/System:	Child strength data
Office/Directorate:	ESHF
Date:	March 19, 2021
A. CONTACT INFORMATION	
Person completing PTA/PIA: (Name, title, organization)	Kristen Talcott, Human Factors Engineer, ESHF
System Owner: (Name, title, organization)	Kristen Talcott, Human Factors Engineer, ESHF
System Manager/Technical POC: (Name, title, organization)	Kristen Talcott, Human Factors Engineer, ESHF

B. APPROVING OFFICIALS

KRISTEN TALCOTT Digitally signed by KRISTEN TALCOTT Date: 2021.03.19 15:18:33 -04'00'

System Owner — March 19, 2021 Date

Senteria Jones Digitally signed by Senteria Jones Date: 2021.04.07 15:26:49 -04'00'

Privacy Officer — April 7, 2021 Date

PATRICK MANLEY Digitally signed by PATRICK MANLEY Date: 2021.04.07 16:15:13 -04'00'

Chief Information Security Officer (CISO) — 4/7/2021 Date

Abioye Mosheim Digitally signed by Abioye Mosheim Date: 2021.04.07 13:20:03 -04'00'

Asst. General Counsel for FOIA, Records and Privacy — April 7, 2021 Date

JAMES ROLFES Digitally signed by JAMES ROLFES Date: 2021.04.08 09:50:25 -04'00'

Senior Agency Official for Privacy (SAOP) — 4/8/2021 Date

C. SYSTEM OF RECORDS NOTICE

1. Will the system or application maintain records that contain information about individuals? Yes ☐ No ☑

2. Will the system or application allow records to be retrieved by a personal identifier*? Yes ☐ No ☑

If the answer to both 1 and 2 above is "Yes," then the system requires a System of Records Notice (SORN).

* *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.*

D. PRIVACY THRESHOLD ANALYSIS (PTA)

1. Will the information system, application, or data set be used to collect, store, or transmit personally identifiable information?	Yes ☐	No ☑
2. Has a Privacy Impact Assessment ever been performed for the information system or application?	Yes ☐	No ☑
3. Is there a Privacy Act System of Records Notice (SORN) for this information system or application?	Yes ☐	No ☑

If ***any*** of the answers to question 1-3 are "Yes" then complete the Privacy Impact Assessment section (F) of this document. If answers to questions 1-3 are all "No" then a Privacy Impact Assessment is not needed. Please complete the section (E) below, sign form, and return to the CPSC Privacy Officer.

E. OMISSION OF A PRIVACY IMPACT ASSESSMENT (PIA)

Briefly describe the system and provide a supporting statement that explains why the PIA is not needed.	The University of Michigan is conducting a study on child strength for CPSC, under contract 61320619F1015/61320618D0004. As part of this study, University of Michigan researchers will collect child anthropometric measurements, demographic information, body scans, and data on the forces that children can apply to test fixtures. Data collection may also include pictures and videos. University of Michigan will conduct the research in accordance with the policies of their Institutional Review Board (IRB), which governs human subject research and protection of participant data, including privacy. Under the contract, University of Michigan will provide data to CPSC

F. PRIVACY IMPACT ASSESSMENT (PIA)

1. Generally describe the type of information that will be collected, stored, or transmitted.	
2. What categories of individuals are covered in the system? (public, employees, contractors)	

G. SYSTEM DATA

3. Is the PII collected verified for accuracy? Why or why not?	
4. Is the PII current? How is this determined?	
5. Who will be responsible for protecting the privacy of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability?	
6. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	
7. 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?	
H. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
8. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	
9. 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.	

10. 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?	
11. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?	
12. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)?	
13. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	
I. ACCESS TO DATA	
14. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	
15. What controls are in place to prevent unauthorized access to the data?	
16. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access?	

17. Is access to the PII being monitored, tracked, or recorded?	
18. 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?	
19. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared?	
20. What CPSC personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)?	
21. Will any of the personally identifiable information be accessed remotely or physically removed?	