United States
Consumer Product Safety Commission

Privacy Threat Analysis (PTA)/Privacy Impact Assessment (PIA)	
Name of Application/System:	Repository of Software Attestation
Office/Directorate of System Owners:	Office of Information and Technology Services (EXIT)
Office/Directorate of Business Owners:	EXIT
Date:	June 24, 2024
A. Contact Information	
Person Completing PTA/PIA: (Name, title, organization)	Caitlyn Borghi, Chief Privacy Officer, EXIT Arlene Clyburn-Miller, Capital Planning and Investment Control (CPIC) Manager, EXIT David Pittman, Funds Control Officer, EXIT
System Owner: (Name, title, organization)	Arlene Clyburn-Miller, Capital Planning and Investment Control (CPIC) Manager, EXIT
System Manager/Technical POC: (Name, title, organization)	David Pittman, Funds Control Officer, EXIT
B. Approving Officials	
Arlene Clyburn-Miller	Digitally signed by Arlene Clyburn-Miller Date: 2024.07.03 11:15:53 -04'00'
System Owner	
CAITLYN BORGHI	Digitally signed by CAITLYN BORGHI Date: 2024.07.03 11:20:28 -04'00'
Chief Privacy Officer (CPO)	
KHALID NUMAN AL-HASSAN	Digitally signed by KHALID NUMAN AL-HASSAN Date: 2024.07.03 11:39:37 -04'00'
Chief Information Security Officer (CISO)	
ABIOYE MOSHEIM OYEWOLE	Digitally signed by ABIOYE MOSHEIM OYEWOLE Date: 2024.07.03 12:56:14 -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: 2024.07.05 10:36:28 -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)	No.
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)	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.	
F. Privacy Impact Assessment (PIA)	

8. Generally describe the type of information that will be collected, stored, or transmitted.	Pursuant to Office of Management and Budget (OMB) Memoranda M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* and M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, CPSC is required to obtain attestation from software producers that their software complies with Government-specified minimum secure software development practices. CPSC will collect information about the software CPSC uses, such as product name(s), version number(s), and release dates; software producer information, such as company name, address, and website; primary contact information, such as name, title, address, phone number, and email address; and the signature, name, and title of the company's Chief Executive Officer or another designee with authority to bind the corporation. CPSC will be collecting this information using the Department of Homeland Security's (DHS) Secure Software Development Attestation Common Form. CPSC's use of this form has been approved by OMB under OMB Control Number 1670-0052. CPSC will email software producers the blank form and receive the forms back via email. The forms will be stored in CPSC's Repository of Software Attestation SharePoint site. CPSC will also be downloading Secure Software Development Attestation Forms from the DHS repository of forms; forms in the DHS repository have been collected by other Federal Government agencies.
9. What categories of individuals are covered in the system? (For example, public, employees, contractors)	The categories of individuals covered in the system are producers of software used by CPSC. CPSC will be collecting information from approximately 149 software producers.
10. Is the personally identifiable information (PII) collected verified for accuracy? Why or why not?	CPSC may work with software producers to verify the software information provided in the Secure Software Development Attestation form, but CPSC will not be verifying any other information collected using the form.
11. Is the PII current? How is this determined?	The initial information collection will be current, as CPSC is obtaining responses directly from software producers in FY24. After initial collection, software producers are responsible for alerting CPSC to any changes in their software development

	practices that would require CPSC to remove their attestation from CPSC's repository.
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?	EXIT staff members and CPSC Contracting Officer's Representatives (CORs) are responsible for protecting the privacy of the software producers whose information will be maintained in the CPSC Repository of Software Attestation SharePoint site. EXIT is developing a standard operating procedure that documents responsibilities for the software attestation process.
13. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	CPSC will be collecting information directly from software producers. We do not anticipate that the CPSC Repository of Software Attestation SharePoint site will contain inaccurate information. However, software producers can submit a Privacy Act Request to obtain access to their own information by contacting the Assistant General Counsel for FOIA, Privacy, and Records at cpscfoiarequests@cpsc.gov or the Chief Information Officer at privacy@cpsc.gov.
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 will collect information directly from software producers. When CPSC takes forms from the DHS repository, information in those forms will have been collected directly from the software producers as well.
15. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Software producers may decline to provide information to CPSC. In the event software producers decline to provide attestation, CPSC will either discontinue use or stop procurement of the software. If software producers are willing to provide information, but unable to attest to the Government-specified minimum secure software development practices, the software producer can work with CPSC to address any issues or deficiencies.
16. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain	No other systems connect to the CPSC Repository of Software Attestation SharePoint site. However, CPSC will pull forms from the DHS repository. CPSC will also share forms it collects with the DHS repository. Sharing of forms with DHS will reduce duplication in the process of collecting information from software producers.

the purpose for system to system transmission, access, or sharing of PII.	
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?	No contractors have been or will be involved in the design or maintenance of the Repository of Software Attestation SharePoint site.
18. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?	Per OMB guidance, CPSC must retain forms or have access to forms for software it uses for the duration of its use, unless the software producer posts a self-attestation publicly and provides a link of the posting to CPSC. The Secure Software Development Attestation forms are covered by DAA-GRS2013-00050010.
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)	The Secure Software Development Attestation forms are temporary records. CPSC will delete forms from its Repository of Software Attestation SharePoint site 5 years after CPSC stops use of the software.
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	EXIT staff will have access to the forms in the Repository of Software Attestation SharePoint site. CORs from other program

the system? (For example, contractors, managers, system administrators, developers, other)	offices within CPSC may assist EXIT in the Secure Software Development Attestation form collection process.
22. What controls are in place to prevent unauthorized access to the data?	Forms are stored in the Repository of Software Attestation SharePoint site where access is restricted to only those individuals with a need-to-know. Access to the SharePoint site is granted by the System Owner and/or the System Manager/Technical POC. SharePoint maintains logs of user activities on SharePoint sites. EXIT staff can request logs for the Repository of Software Attestation SharePoint site as needed.
23. What controls are in place to prevent the misuse of PII by those having access?	EXIT staff are required to take security and privacy awareness training and sign a Rules of Behavior document upon joining CPSC and annually thereafter. SharePoint maintains logs of user activities on SharePoint sites. EXIT staff can request logs for the Repository of Software Attestation SharePoint site as needed.
24. Is access to the PII being monitored, tracked, or recorded?	Yes, access to the PII is being recorded. EXIT staff can request logs for the Repository of Software Attestation SharePoint site as needed.
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 the Repository of Software Attestation SharePoint site is controlled by the System Owner and/or the System Manager/Technical POC. Individuals wishing to access the Repository must request permission. EXIT is developing a standard operating procedure documenting criteria and procedures for determining which individuals should be involved in the collection process and who should be granted access to the Repository of Software Attestation SharePoint site.
26. What third-party organizations will have access to the PII? Who establishes criteria for what PII can be shared?	Forms will be shared with other Federal Government agencies via the DHS repository. CPSC intends to share as many forms as possible with the repository to avoid unnecessary collection and duplication of information.
27. What CPSC personnel roles will	The System Manager, the System Manager/Technical POC, and staff from the Information Technology Security Office and

have access to PII fields? (For example, users, managers, system administrators, developers, contractors, other)	program office CORs conducting this collection will have access to the PII.
28. Will any of the PII be accessed remotely or physically removed?	Forms may be duplicated and shared with the DHS repository as necessary.