U.S. Consumer Product Safety Commission Office of Inspector General PRIVACY IMPACT ASSESSMENT	
Name of Project:	WDesk
Office/Directorate:	Office of Inspector General
A. CONTACT INFORMATION	
Person completing PIA: (Name, title, organization and ext.)	Daniel Burrows, IT Auditor, CPSC OIG, x7610
System Owner: (Name, title, organization and ext.)	Christopher W. Dentel, Inspector General, CPSC OIG, x7644
System Champion: (Name, title, organization and ext.)	Daniel Burrows, IT Auditor, CPSC OIG, x7610
B. APPROVING OFFICIALS	**Signature/Date**
System Owner/ Senior Official for Privacy/Reviewing Official Christopher W. Dentel, IG, CPSC OIG System of Record? Yes x No	X CHRISTOPHER DENTEL Digitally signed by CHRISTOPHER DENTEL Date: 2021.07.18 08:03:44 -04'00'
WDesk Champion/Privacy Advocate Daniel Burrows, WDesk Champion, CPSC OIG	X Daniel Burrows Digitally signed by Daniel Burrows Date: 2021.07.14 14:19:20 -04'00'
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, volunteers, and contractors
2. Generally describe what data/information will be collected in the system.	WDesk houses all of the OIG audit data and information. OIG audit data and information, etc, is generated/provided by the CPSC. As such, all CPSC data could potentially be collected and maintained in WDesk. WDesk may contain Public individuals' birth dates, addresses, emails, health data, geographic data, gender, financial, human resource, and salary 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?	Personal information will generally not be collected directly from individual members of the public. The primary source of the information will be the CPSC. Additional information may be collected from CPSC contractors or other government organizations. Generally, this information will be collected from audit or investigation liaisons . However, the data may also be provided by nongovernmental sources, such as , public safety entities, manufactures, etc... as required.
4. How will data be checked for completeness and accuracy?	Audit results require manual review by an independent source (ex. the Deputy Inspector General) and both the preparer and reviewer must certify the accuracy, relevance, timeliness, and completeness of the information. Inaccurate data may need to be stored to provide support for an audit or investigation – however, if it is stored, then the working papers associated with the documentation will indicate the

	information is inaccurate.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	As WDesk is a document repository for all audit work, not all data in WDesk is current. The OIG has developed and follows its internal records disposition policy and schedule and is having its schedule reviewed by the National Archive and Records Administration requirements for approval.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	The agency collects all (39 in total) types of "Services Delivery Support Information" outlined in NIST SP 800-60, except for, Executive Function, Federal Asset Sales, and Tax and Fiscal Policy and all of the data types are documented and detailed in the WDesk system security plan.,.
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 OIG uses the data within WDesk to support the mission by identifying fraud, waste, and abuse as well to as to provides value-added recommendations to management.
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.	WDesk is categorized as a moderate impact system and is subject to all controls outlined for moderate impact systems in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. Most of WDesk security controls are common controls, and WDesk cloud infrastructure (hosted by Workiva) and these controls rely on Workiva's network database, and most application security controls for security. However, OIG management has configured WDesk to implement the Principle of Least Access, Segregation of Duties, and monitoring logs of user access at the application level. For example, all WDesk users with access to a project can view logs that include the name and last login data of all users that have logged into a project. Also, according to vendor documentation (WDesk FedRAMP certification package), WDesk's encryption has been tested and leverages FIPS cryptography 140-2 as well as has implemented all requisite common controls.
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.	WDesk users (OIG members) access the data through the application using multifactor authentication via Personal Identity Verification cards. Workiva administrators also can access the data. However, all activity is logged. Data is neither organized nor retrieved by personal identifiers.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	N/A
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	All audit records are archived until the OIG's retention schedule has been approved by NARA.
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 the procedures documented?	N/A. See above.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	WDesk is secured using PIV Authentication. All WDesk users have completed the annual security awareness training and certified the annual CPSC Rules of Behavior and IG Rules of Behavior documents that outline user responsibilities in regards to handling CPSC and OIG data. WDesk is FIPS 140-2 compliant. Also, as mentioned before, the Workiva cloud administrators have sufficient access to monitor WDesk data and transactions, however, activity is logged at the WDesk application level.

5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No. A system of record is an information storage and retrieval system that is the authoritative source for a particular data element in a system containing multiple sources of the same element. As an audit workpaper editor and data repository, WDesk does not act as an authoritative source for any particular data element.
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	N/A. This is the first PIA documented and WDesk is not a System of Records.
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	Only OIG staff and Workiva cloud administrators with a need to know have access to the data in the system. OIG auditors from other agencies are provided with copies of data housed in WDesk to perform peer audit reviews. CPSC resources may be provided with read/upload access to WDesk to provide responses to IG requests – however, CPSC resources do not have access to modify data within WDesk or to view information that is not related to the requests made.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	WDesk utilizes PIV authentication. Also, all WDesk users have completed the annual security awareness training and certified the annual CPSC Rules of Behavior and OIG Rules of Behavior documents that outline user responsibilities in regards to handling CPSC and OIG data.
3. Who is responsible for assuring proper use of the data?	The system security organization consisting of the WDesk Champion (and privacy advocate) and WDesk system owner (and SAOP).
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?	WDesk is a FedRAMP certified commercial-off-the-shelf cloud solution hosted by Workiva. Also, Workiva provides ongoing support for WDesk and as part of the troubleshooting process may have access to the data collected by the system. However, as this is not a System Of Records, Federal Acquisition Regulation (section 24.102) does not require the inclusion of Privacy Act clauses in the WDesk 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?	No.
6. Will other agencies share data or have access to the data in this system? If yes, how will the data be used by the other agency?	Other federal OIGs will have access to the data collected in WDesk as part of the peer review process.
7. Will any of the personally identifiable information be accessed remotely or physically removed?	Yes. Remote access is permitted as this is a cloud solution. However, none of the WDesk data will be physically removed.