Affects Members Of the Public? Mark if Applicable w/ an X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: ***https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	July 25, 2024
Departmental Element & Site	Infrastructure Operations Office, IM-61
Name of Information System or IT Project	Kiteworks Software as a Service (SaaS) provided by Kiteworks and built upon Amazon Web Services (AWS) infrastructure as a Service (IaaS).
Exhibit Project UID	019-000001955
New PIA ☐ **Update** ☒	Adopted New template and Periodic update to the approved 1/27/2023 Kiteworks PIA with no material changes to the system.

	Name, Title	Contact Information Phone, Email
System Owner	LaQuan Ippolito Kiteworks System Owner Infrastructure Operations Office, IM-61	301-903-8673 Laquan.ippolito@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-40	privacy@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Manda Shu-Nyamboli, ISSO Security and Compliance, IM-63 ISSO	301-903-0102 Manda.shu-nyamboli@hq.doe.gov
Person Completing this Document	Travis Walter Technical Point of Contact, IM-61	301-903-6278 Travis.walter@hq.doe.gov
Purpose of Information System or IT Project	The Kiteworks is a file sharing web application for use by EITS customers. It enables secure anytime, anywhere access to information on public, private/on-premises, and hybrid clouds, while ensuring enterprise security and compliance. Robust features allow authorized and validated users to access and share the latest files and folders on smartphones, tablets, laptops, and desktops. End-to-end security ensures files are synchronized, uploaded, downloaded, and shared securely. Kiteworks is built on Amazon Web Services Infrastructure as a Service (IaaS), located at Kiteworks.doe.gov. The system collects the following PII, which is used for the administration of the system: display name (DOE email), User Id (DOE email), business email address, and mobile device type. Optionally, individuals may enter the following administrative PII: name, organization, title, and role. In addition, the system allows for the uploading of any file in DOE for sharing. Files uploaded into Kiteworks system are not readable to the system. Files are encrypted at rest and in transit and are only readable to the intended parties. The Kiteworks enables seamless uploading of any files with DOE, facilitating internal and external sharing. Consequently, due to the potentially limitless number of external partners, Kiteworks is unable to establish specific agreements with each recipient. Furthermore, Kiteworks do not impose any restrictions on the nature of the content shared. It is important to note that Kiteworks operates as a FISMA Moderate System, indicating its suitability for handling sensitive information such as PII and CUI.	
Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☐ Name, Phone, Address ☒ Other – Please Specify: Display Name (DOE email), Userid (DOE email), Business Email Address, and Mobile Device Type. Optional data is: (if the user elects to provide) First Name, Last Name, Signature, Organization, Title, and Role. Kiteworks allows any file in DOE to be uploaded for sharing inside and outside of the agency.
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	PII exists
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES

MODULE I – PRIVACY NEEDS ASSESSMENT

3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	• 10 CFR § 1008 • 42 USC § 7101

MODULE II – PII SYSTEMS & PROJECTS	
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Kiteworks is designed to be a secure application to upload, download, and securely share large files. Content shared, uploaded, or downloaded is the responsibility of the data owner(s). Kiteworks does not enforce any content filtering on files being uploaded or downloaded to or from the users. (Customers are notified that Kiteworks is not a data repository. Kiteworks data is considered transitory data). Administrative PII for user accounts is a requisite of use of the system.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	The Kiteworks vendor is responsible for maintaining the platform and design of the system. DOE is responsible for further maintenance and development as well as maintaining the user account information.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The privacy impact of the system is moderate. Kiteworks only requires the user to provide low sensitivity administrative PII. The login warning banner reminds user to not upload sensitive privacy data into the system. Should users follow system guidance, the impact on privacy is minimized. In addition, risks are mitigated via a series of technical, administrative, and physical controls. Files uploaded to the Kiteworks system are not readable to Kiteworks. Files are encrypted at rest and in transit and only readable to the intended parties. Should the administrative PII required by the system be compromised, the privacy harm to individuals would be minimal. A compromise of this PII could damage the trust between employees and their employer and result in minor professional harm and embarrassment. Should users upload sensitive PII into Kiteworks and should that data be compromised, the potential harm to individuals could be severe, depending on the information and its sensitivity. Kiteworks observes a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). Kiteworks maintains the minimum PII necessary for its business purpose to mitigate privacy harm. Access to and use of data in the system is protected by a series of controls including role and permission-based monitoring controls.

MODULE II – PII SYSTEMS & PROJECTS	
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Data is retrieved by file name and not by unique identifier.
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	N/A
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Individuals
9. Will the information system derive new or meta data about an individual from the information collected?	No Files uploaded to the Kiteworks system are not readable to Kiteworks. Files are encrypted at rest and in transit and only readable to the intended parties.
10. Are the data elements described in detail and documented?	Yes

MODULE II – PII SYSTEMS & PROJECTS	
DATA USE	
11. How will the PII be used?	Administrative PII is used for account setup and system access. Kiteworks is a secure file sharing application. The application does not use information uploaded to it. The application only shares the uploaded data to approved and authorized parties. Use of data uploaded to the system is the responsibility of users.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	N/A
13. With what other agencies or entities will an individual's information be shared?	The application does not share PII with any other agency.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The only reports produced by Kiteworks consist of audit logs used to maintain the security and integrity of the system.
15. What will be the use of these reports?	For auditing purposes, logging user login attempts, storage used, bandwidth used and system health such as storage capacity monitoring.
16. Who will have access to these reports?	System administrators.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Individuals are not tracked or monitored by the system. Only user activity on the system is logged and tracked for system auditing purposes.
18. What kinds of information are collected as a function of the monitoring of individuals?	The system does not facilitate the monitoring of individuals.

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system employs physical, administrative, and technical controls. Role-based access controls restrict access to data based on job function. Files uploaded Kiteworks system are not readable to the system. Files are encrypted at rest and in transit and only readable to the intended parties.
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	Data uploaded to the system is the responsibility of users and data owners.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Kiteworks is a centralized secure file sharing application wherein users can upload files to share with specific individuals. The data owner is responsible for the data that is uploaded to the system and its use.
Records Management	
22. Identify the record(s).	System access records, non-recordkeeping copies of electronic records.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled ☐ Scheduled *(cite NARA authority(ies) below)* Not applicable to Kiteworks Transitory data
24. Records Contact	Virginia Elharam Virginia.elharam@hq.doe.gov 301-903-1468
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system employs physical, administrative, and technical controls. Role-based access controls restrict access to data based on job function. Files uploaded Kiteworks system are not readable to the system. Files are encrypted at rest and in transit and only readable to the intended parties.
26. Who will have access to PII data?	Users have access to files they upload, and files shared with them. Administrators have access to audit logs and user data based on a need-to-know. Administrators cannot access or read files uploaded by users.
27. How is access to PII data determined?	Users may control access to files they upload by sending an invitation and a link to the file. System administrators can delete the file but cannot access or read the file.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	The information owners upload files to Kiteworks and control access to uploaded files.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**LaQuan Ippolito** **(Print Name)** LAQUAN IPPOLITO Digitally signed by LAQUAN IPPOLITO Date: 2024.08.29 11:25:36 -04'00' **(Signature)**	
Local Privacy Act Officer	**(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.08.28 10:36:56 -04'00' **(Signature)**	
Chief Privacy Officer	**Ken Hunt** **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.08.28 10:37:16 -04'00' **(Signature)**	