Template Version Number: 01-2022

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment (PIA)
for the
KITEWORKS Secure File Transfer (SFT)

Reviewed by: ___Tiffany Daniel_____, Bureau Chief Privacy Officer (BCPO)

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.05.08 11:50:24 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date
(Or the BCPO if this is an existing system that is eligible for an annual certification)

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary/Kiteworks

Unique Project Identifier: 2640

Introduction: System Description

Provide a brief description of the information system.

Kiteworks Secure File Transfer (SFT) is a web portal available to Department of Commerce (DOC) internal and external customers that allows a secure exchange of files between users and the service configured in a multi-tier architecture. The service is made available to DOC Users (Federal and Contractors) and external users for uploading files for secure transfer to other registered account users. Kiteworks enables the DOC to securely connect all its content to the people and systems that are part of their critical business processes, regardless of the applications that create that content or where it is stored.

Kiteworks collects a user's email address and password to register as an account on the Host Server to perform secure file transfer. Additionally, DOC users have the option to use the Integrated Database Management System (IDMS) through Personal Identity Verification (PIV) for authentication. All user files uploaded for secure transfer are encrypted and temporarily stored in the user's storage space for a limited time. Since the files are encrypted throughout the storage and transfer process, the confidentiality of the information is kept secure from any attempts to view the file other than the user and recipient where the file is unencrypted at the user's endpoint device. The temporary files have a limited duration for storage and are purged during regular maintenance cycles.

Kiteworks has no requirement to collect any type of PII other than the username and Password, and this data is used for continuous monitoring purposes only. There is a 30-day expiration for data shared via e-mail and a 90-day expiration for data shared via the folders created and shared within the system. This solution does not control the type of data uploaded and saved by its users. Therefore, multiple Department of Commerce System of Record Notices (SORNs) are identified for which the system may be covered.

Address the following elements:

(a) *Whether it is a general support system, major application, or other type of system.*
This system is a Major Application

(b) *System location:*
Kiteworks Federal Cloud manages the system in the AWS East and West regions. The system is located on the vendor FedRAMP cloud platform Amazon Web Services (AWS).

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

This system is a Software as a Service (SaaS) solution and does not have any interconnections with other applications.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Kiteworks is a web portal available to DOC internal and external customers that allows a secure exchange of files between users and the service configured in a multi-tier architecture. The service is made available to DOC users for uploading files for secure transfer to other registered account users.

Kiteworks only collects a user's email address and password to register as an account on the Host Server to perform secure file transfer. All user files uploaded for secure transfer are encrypted and temporarily stored in the user's storage space for a limited time. Since the files are encrypted throughout the storage and transfer process, the confidentiality of the information is kept secure from any attempts to view the file other than the user and recipient where the file is unencrypted at the user's endpoint device. The temporary files have a limited duration for storage and purged during regular maintenance cycles.

(e) How information in the system is retrieved by the user

1. Users are notified by email from the system that a file has been uploaded for transfer.
2. The user retrieves the file by logging into their account mailbox and securely downloads the file ready for transfer.

(f) How information is transmitted to and from the system

1. A user logs into his/her account on the web server.
2. The user then uploads a file and writes an optional message to the recipients.
3. The user selects a send button from their account for the file and the message that is securely sent to the recipient(s). Only recipients with an account can open the file.

(g) Any information sharing

There is no information sharing that occurs from system to system. Information sharing only occurs between end users (sender/receiver), through a secured environment with FIPS 140-2 encryption.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, as required by the Federal Information Security Modernization Act (FISMA) of 2014; Title 5 U.S.C.; Title 31 U.S.C. 66a, 492; 32 CFR § 2002.16; Homeland Security Presidential Directive 12 (HSPD-12).

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system: Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X__ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

____ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): The system does not automatically collect any personally identifiable information (PII). However, if sensitive data, including an identifying number, is required for a specific task, this information may be intentionally collected and shared between end users only for that purpose.					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): The system does not require the collection of general personal data for its operation or use. However, it is designed to support the sharing of sensitive Controlled Unclassified Information (CUI). In such cases, the data exchanged between end users may include identifying numbers, depending on the specific requirements of the task for which the information is being shared.					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): The system does not require the collection of work-related data for its operation or use. However, it is designed to support the sharing of sensitive CUI. In such cases, the data exchanged between end users may include work-related data, depending on the specific requirements of the task for which the information is being shared.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): The system does not require the collection of distinguishing features/biometrics for its operation or use. However, it is designed to support the sharing of sensitive CUI. In such cases, the data exchanged between end users may include distinguishing features/biometrics, depending on the specific requirements of the task for which the information is being shared.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email	X		
Other (specify): Documents typically sent via physical mail, faxes or other original or copied documents are scanned and uploaded and may be attached to emails. Although these hard copy documents are part of the process, they are shared digitally through email as attachments, rather than being sent through traditional U.S. Mail.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify):					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Kiteworks ensures the accuracy, integrity, and confidentiality of information through strong authentication, encryption, and access controls. Organizational users authenticate via Single Sign-On (SSO) through the National Oceanic and Atmospheric Administration's (NOAA) Identity, Credential, and Access Management system (ICAM) portal or Okta, while external users register with email-based authentication.
The system enforces automatic session timeouts (30 minutes), account lockouts after five failed login attempts, and deactivation of inactive accounts after 30 days.

Uploaded files are encrypted at rest and in transit, ensuring that only the sender and designated recipient can access the decrypted data at the user's endpoint. Files are temporarily stored in the user's storage space for a limited time and automatically purged during regular maintenance cycles. Audit logs track all system activities and are forwarded to the DOC Security Operations Center (SOC) Splunk system for monitoring and anomaly detection.

Accuracy and confidentiality are core components of the Privacy Impact Assessment (PIA), with Kiteworks enforcing encryption and least privileged access to protecting sensitive data. Separation of duties prevents unauthorized modifications, and strict access controls ensure that only authorized users can make system changes. No external system interconnections or portable storage devices are permitted without explicit approval, reducing security risks. These measures, aligned with NIST 800-53 guidelines, establish a multi-layered security framework that safeguards information throughout authentication, storage, and secure transmission.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.

X	No, the information is not covered by the Paperwork Reduction Act. The information is not covered by the Paperwork Reduction Act (PRA) because Kiteworks does not collect information from the public for agency use, nor does it require the submission of structured data for reporting or recordkeeping purposes. The system functions solely as a secure file transfer platform, enabling the electronic transmission of Controlled Unclassified Information (CUI), PII, and BII between authorized users. While Kiteworks facilitates the exchange of sensitive information, it does not actively collect, manage, or maintain records beyond temporary encrypted file transfers. The system does not store data permanently, and all files are automatically purged after 90 days. Given that no structured information collection occurs that falls under PRA requirements, there is no applicable OMB control number for this system. Thus, Kiteworks is not subject to PRA reporting obligations, as its primary function is to provide a secure means for users to transmit files, rather than collect or manage data for federal information collection purposes.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single session)		For web measurement and customization technologies (multi-session)	
Other (specify): Kiteworks does not collect personally identifiable information (PII) or business identifiable information (BII). However, it serves as a secure platform for sharing documentation that may contain various data types, including sensitive PII and/or BII. The type of information shared depends on the specific purpose defined by each end user.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Kiteworks facilitates the secure sharing of various data types, which may include sensitive PII and BII, depending on the needs of the end user. The platform supports business processes related to IT systems, human resources, contractual agreements, and other departmental operations that require the exchange of confidential or sensitive information. The type of PII/BII shared is determined by the end user and may pertain to federal employees, contractors, members of the public, foreign nationals, or visitors, as applicable to the specific use.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is a potential risk of insider threats and unauthorized disclosure of sensitive information. To mitigate these risks, system administrators actively monitor user activity logs to detect any suspicious behavior. Additionally, while documents shared through Kiteworks are encrypted at rest and in transit, there remains a risk that sensitive information may be included in the body of a message, which may not be encrypted unless full message encryption is selected.

To ensure proper handling and protection of information, all department users are required to complete mandatory cybersecurity and privacy awareness training. Furthermore, automated data retention controls are in place to purge temporary files during regular maintenance cycles, ensuring that information is appropriately managed and disposed of in accordance with security policies.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus			X
Federal agencies			X
State, local, tribal gov't agencies	X		
Public	X		
Private sector	X		
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. Users in Kiteworks do not have the authority to forward emails or shared files directly to external recipients outside the DOC without approval. The system enforces strict access controls and encryption, ensuring that only the intended recipient can access shared data. Additionally, external entities receiving PII/BII through Kiteworks must obtain verification from the DOC bureau/operating unit before re-disseminating any shared information. The system's audit logging mechanisms track access and file sharing activities, enabling oversight, monitoring and enforcement of compliance with DOC security policies. Yes, the DOC bureau/operating unit places limitations on the re-dissemination of PII/BII shared with external agencies or entities. External recipients must obtain verification and approval from the DOC bureau/operating unit before further sharing any PII/BII received through Kiteworks. This ensures that sensitive information is used only for its intended purpose and remains protected in compliance with privacy, security, and regulatory requirements. Additionally, Kiteworks enforces encryption for all file transfers and implements access controls based on the least privilege principles, reducing the risk of unauthorized dissemination.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

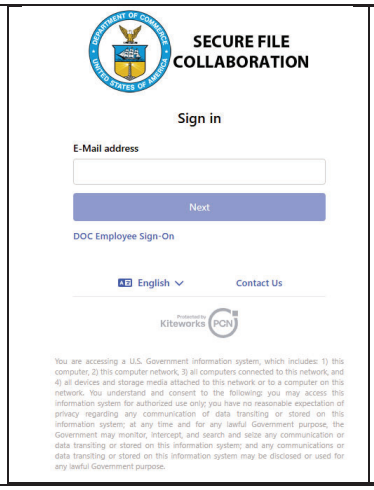
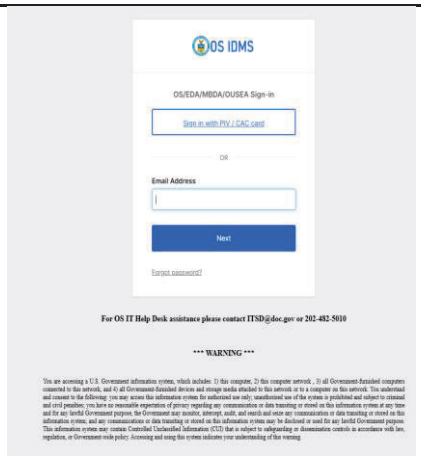
6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sfc.doc.gov/#/

	 	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Yes, individuals can decline providing PII/BII. When accessing Kiteworks, users are presented with a government system warning banner informing them that all activities may be monitored, and data may be intercepted, searched, or used for lawful government purposes. By proceeding with login, individuals acknowledge and consent to these terms before transmitting any information. Kiteworks privacy policy https://sfc.doc.gov/#/ Users are not required to use Kiteworks and may choose alternative secure DOC-approved methods for transmitting sensitive data, such as encrypted email, secure FTP, or other federally compliant platforms. This ensures that individuals have full control over how their information is transmitted, while also maintaining compliance with DOC security and privacy policies.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Yes, individuals can consent to uses of their PII/BII before sharing it through Kiteworks. Upon accessing the system, users are presented with a U.S. Government system warning banner, which explicitly informs them that their data may be monitored, intercepted, searched, and used for lawful

		government purposes. By proceeding with the login, individuals acknowledge and consent to these terms, ensuring they are aware of how their information may be used. Users are not required to use Kiteworks and may opt for other secure, DOC-approved methods for transmitting sensitive data, such as encrypted email, secure FTP, or alternative federally compliant platforms. If individuals choose to proceed with Kiteworks, they accept that their activities may be monitored and logged as part of security and compliance measures. This approach ensures transparency and alignment with DOC security and privacy requirements.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Yes, individuals have an opportunity to review and update PII/BII before sharing it via Kiteworks. Since Kiteworks does not collect or store PII/BII beyond temporary encrypted file transfers, users maintain full control over the information they choose to upload and share. Before submitting any files, individuals can review, edit, or update their documents to ensure accuracy and completeness. Additionally, users are required to authenticate via NOAA ICAM or Okta before accessing Kiteworks, ensuring that only authorized individuals can manage their data securely. However, once files are uploaded and transmitted, they are encrypted and temporarily stored in accordance with DOC security policies and automatically purged during regular maintenance cycles. Users do not have the ability to modify or retrieve previously shared files once they have been sent. The login warning banner further informs users that all activities on the system may be monitored, intercepted, and audited, reinforcing the importance of reviewing their information before transmission. If users need to update or correct previously shared information, they must resubmit a revised version through Kiteworks or an alternative DOC-approved secure transmission method.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The PII is being tracked and monitored in the form of system access logs and login logs as part of the continuous monitoring efforts.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 06/05/2025 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Kiteworks protects PII/BII using a multi-layered security approach aligned with FIPS 200, NIST 800-53 Rev. 5, and FedRAMP Moderate requirements. The system enforces strong access controls, authentication mechanisms, encryption, and audit logging to safeguard sensitive data.

- Access Control: Single Sign-On (SSO) via NOAA ICAM/Okta, role-based permissions, session limitations, and automated deactivation of inactive accounts.
- Identification & Authentication: Strong authentication is enforced through federated identity management, ensuring only authorized users access the system.
- Audit & Accountability: System logs capture protocol addresses, timestamps, success/failure attempts, and audit trails, enabling monitoring and compliance.
- Data Security: All files are encrypted at rest and in transit by FIPS 140-2 standards. Data remains protected from unauthorized access, and files are only decrypted at the user's endpoint. Temporary files are automatically purged during scheduled maintenance cycles.
- Cryptographic Controls: Kiteworks manages encryption keys and certificates in compliance with federal cryptography policies (FIPS 140-3, Crypto Policy FIPS_140sp3219) for secure key generation, distribution, storage, and destruction.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

__X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: The applicable SORNs have been selected based on the types of Controlled Unclassified Information (CUI), specifically PII and BII, that may be shared through Kiteworks. The following SORN(s) are relevant to the purpose, authority, and data handling scope of this Privacy Impact Assessment (PIA): System of Records Notices | U.S. Department of Commerce **Department-wide Notices** • DEPT-5, Freedom of Information Act and Privacy Act Request Records • DEPT-13, Investigative and Security Records • DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs • DEPT-25, Access Control and Identity Management System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X		There is an approved record control schedule. Provide the name of the record control schedule: Yes, records shared through Kiteworks are covered by an approved records control schedule. The applicable schedule is: Management and Information Systems (N1-040-87-004) Link to National Archives Record Schedule Management and Information Systems Records

		Specific Records Covered Under This Schedule: The Management and Information Systems (N1-040-87-004) schedule applies to various categories of electronic records related to program management, administrative functions, and data exchanges within the Department of Commerce. The specific records covered include: • Electronic records used in information and communication systems, including email and file-sharing systems • Records related to system access, user activities, and security logs • Administrative records supporting program operations • Information systems used to transmit or store sensitive business and personnel-related records.
		No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
		Yes, retention is monitored for compliance to the schedule.
X		No, retention is not monitored for compliance with the schedule. Provide explanation: This schedule governs the management and retention of electronic records within the Department of Commerce, including those used for data transmission and secure file sharing. However, Kiteworks does not serve as a long-term records management system. The platform is primarily used to facilitate the secure transmission of sensitive information, including PII and BII, across various program offices. While program offices may apply specific records retention schedules to their own data, Kiteworks itself does not maintain records beyond its automated storage timeframe. • Retention Policy on Kiteworks: o All files stored in Kiteworks are automatically deleted permanently after 90 days of non-use. o Files are not archived or backed up for long-term records management. o Once deleted, files cannot be recovered, ensuring compliance with security and privacy requirements. Compliance Monitoring: Since Kiteworks is not a records repository, retention is not actively monitored for compliance with the records schedule within the system itself, as files are systematically purged to prevent unauthorized data retention. Instead, program offices that use Kiteworks must apply their own records retention policies to ensure compliance with federal and departmental records management requirements.

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify): Information is eliminated after the period for retreat of information has expired.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Information sent via Kiteworks may contain PII about the sender or receiver. Additionally, the body of an email is searchable by any word included, not just sender or receiver details, which could increase the risk of inadvertent exposure. While email bodies and attachments are encrypted, contextual clues in unencrypted metadata, such as email subject lines, could still reveal sensitive details.
X	Quantity of PII	Provide explanation: Kiteworks facilitates secure file sharing across multiple users and program offices within the Department, leading to a significant volume of stored information at any given time. Due to its federated use across various divisions, PII/BII from diverse groups of users may be transmitted through the system, necessitating strong security controls to maintain confidentiality.
X	Data Field Sensitivity	Provide explanation: Although all user files and email contents are encrypted at rest and in transit per FIPS 140-2 standards, there are still potential risks. The subject line of an email remains unencrypted, which may provide contextual clues about the nature of the information being transferred. While Kiteworks ensures that files and email bodies are fully encrypted, users must remain aware that unencrypted metadata (e.g., subject lines) could reveal sensitive information. To mitigate risk, Kiteworks enforces access controls, and temporary files are regularly purged following federal cryptography guidelines.
X	Context of Use	Provide explanation: Kiteworks is used by multiple program offices to transmit sensitive information for various purposes, including: • Auditing and compliance assessments, • Investigations and legal matters, • Evaluation processes, • Human resources personnel processing and management. Due to its broad application, sensitive PII/BII may be handled within different operational contexts, making it critical to always ensure strong confidentiality protections.
X	Obligation to Protect Confidentiality	Provide explanation: As a federal system facilitating secure data transfers, Kiteworks is obligated to protect PII/BII confidentiality. The Department enforces strict encryption protocols, access

		control mechanisms, and system monitoring to safeguard sensitive data. The diverse user base, including government employees, contractors, and external partners, further increases the need for consistent security enforcement to prevent unauthorized access or disclosure.
X	Access to and Location of PII	Provide explanation: Kiteworks operates as a secure cloud-based solution, allowing users to transmit and store encrypted files temporarily. All file transfers and stored data are encrypted by federally approved cryptography guidelines. However, access to this information is restricted based on authentication policies, ensuring only authorized users can retrieve and decrypt shared data.
	Other:	Provide explanation: After authentication, files uploaded to Kiteworks for secure transfer are encrypted and temporarily stored on the user's storage space for a limited duration. Since the files are encrypted throughout both storage and transfer, only the sender and designated recipient can access the decrypted information at the user's endpoint. Temporary files are automatically purged during regular maintenance cycles, further reducing the risk of unauthorized access.

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There are potential threats to privacy in the collection, transmission, and storage of sensitive information within Kiteworks. The primary risks include insider threats, unauthorized disclosure, and data exposure through unencrypted metadata. To mitigate these risks, system administrators actively monitor user logs for suspicious activity, and all users are required to complete mandatory cybersecurity and privacy awareness training.

One key risk is sensitive information being exposed in unencrypted email subject lines, even though email bodies and attachments are encrypted at rest and in transit. If full message encryption is not enabled, the entire message may not be fully protected. Users are advised to avoid including sensitive details in subject lines and to enable full encryption when necessary.

Kiteworks enforces strong authentication via NOAA ICAM or Okta for organizational users and email-based authentication for external users, ensuring controlled access. Although different methods apply based on user type, all authentication mechanisms enforce strict identity verification to protect privacy and prevent unauthorized access.

Additionally, all user files uploaded for secure transfer are encrypted at rest and in transit, ensuring that only the sender and designated recipient can access the decrypted file at the endpoint device. Files are temporarily stored in a secure environment and automatically purged during scheduled maintenance cycles to reduce data exposure. To further mitigate privacy risks, system administrators receive specialized training and must adhere to established rules of behavior, ensuring they understand the importance of safeguarding sensitive information. Mandatory cybersecurity and privacy training is required for all users, reinforcing best practices in handling, transmitting, and protecting sensitive data. These measures significantly reduce the likelihood of privacy breaches and insider threats while ensuring compliance with federal security policies.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.