Version Number: 01-2021

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Kiteworks-Accellion

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 02/16/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

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

Unique Project Identifier:

Introduction: System Description

Provide a brief description of the information system.

Kiteworks-Accellion is a web portal available to the 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-Accellion 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-Accellion 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 on 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.

Kiteworks-Accellion 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 to 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*
Major Application

(b) *System location:*
This system is a Software as a Service (SaaS) solutions hosted 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 solutions does not have any interconnections with other applications.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
Kiteworks-Accellion 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-Accellion 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 on 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 his/her 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 his/her account for the file and the message that is securely sent to the recipient(s). Only recipients with an account can unopen 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.

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 itself does not require any of these identifying numbers to be collected in order to function or be used. However, the system is designed to support the sharing of sensitive controlled unclassified data, the information exchanged between/among end users could contain an identifying number, which is contingent upon the needs task for which the information is being shared.					
*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	
Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): The system itself does not require any of these types of general personal data to be collected in order to function or be used. However, the system is designed to support the sharing of sensitive controlled unclassified data, the information exchanged between/among end users could contain an identifying number, which is contingent upon the needs task for which the information is being shared.					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		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 itself does not require any of these types of work-related data to be collected in order to function or be used. However, the system is designed to support the sharing of sensitive controlled unclassified data, the information exchanged between/among end users could contain an identifying number, which is contingent upon the needs 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 itself does not require any of these distinguishing features/biometrics to be collected in order to function or be used. However, the system is designed to support the sharing of sensitive controlled unclassified data, the information exchanged between/among end users could contain an identifying number, which is contingent upon the needs 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	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
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-Accellion authenticates organizational users, but validates user accounts through SSO authentication via NOAA ICAM portal or via ADFS LDAP (Active Directory Federation Services Lightweight Directory Access Protocol). The Kiteworks-Accellion system passes the token to NOAA ICAM system which in turn, based on the Bureau that the user selects, transfers the user to the appropriate IDP for authentication. The Kiteworks-Accellion system passes the token to ADFS LDAP for authentication where the user's email address and password are used to authenticate the user.

After a user is authenticated, files uploaded for secure transfer are encrypted and temporarily stored on 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.

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.

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 no 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-Accellion does not collect any PII/BII. Kiteworks-Accellion can be used to securely share documentation which may contain any data type, like sensitive PII and/or BII. The information collected is contingent on the purpose identified 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 can be used to securely share any type of data, which may contain sensitive PII and BII. An end user may need to provide documentation related to IT systems, supportive documentation that may be considered confidential or sensitive in nature concerning human resources, contractual information, or any other type of information that supports one of the OS program offices. This information could also be shared with external entities in support of DOC's federal programs. Not only could this include DOC employees, but also federal employees, contractors, and members of the public.

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 the potential for insider threat. There are system administrators who monitor the user logs. There is also the potential for sensitive information to be disclosed in the body of a message, even if the documents shared are encrypted. The entire message, if not selected for full encryption of the message itself, may not be encrypted. All Kiteworks users are required to take mandatory cyber security and privacy awareness training.

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			
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?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	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://sft.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: Kiteworks-Accellion is used to securely share any sensitive data, such as documentation that may contain PII and BII and users have the choice to decline using the system for data sharing.
	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: Users can consent the use of the system and use other secure approved DOC means of sharing information
	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: Users have the liberty to review information before sharing via Kiteworks-Accellion
	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): 12/02/2021 ☐ 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 4 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).*

Accellion establishes and manages cryptographic keys and certificates for the cryptography employed within the kiteworks Federal Cloud system in accordance with Federally approved cryptography guidelines (Crypto Policy FIPS_140sp3219) for key generation, distribution, storage, access, and destruction.

All user files are encrypted per the FIPS 140-2 standards, for 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.

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 below SORNs are listed with the understanding that the end user may upload any type of Controlled Unclassified Information, specifically PII and BII. • DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons • DEPT-2, Accounts Receivable • DEPT-3, Conflict of Interest Records, Appointed Officials • DEPT-4, Congressional Files

	• DEPT-5, Freedom of Information Act and Privacy Act Request Records • DEPT-6, Visitor Logs and Permits for Facilities Under Department Control • DEPT-7, Employee Accident Reports • DEPT-8, Employee Applications for Motor Vehicle Operator's Card • DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons • DEPT-10, Executive Correspondence Files • DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees • DEPT-12, OIG Investigative Records • DEPT-13, Investigative and Security Records • DEPT-14, Litigation, Claims, and Administrative Proceeding Records • DEPT-15, Private Legislation Claimants-Central Legislative Files • DEPT-16, Property Accountability Files • DEPT-17, Records of Cash Receipts • DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies • DEPT-19, Department Mailing Lists • DEPT-20, Biographical Files and Social Networks • DEPT-22, Small Purchase Records • DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs • DEPT-25, Access Control and Identity Management System • DEPT-27, Investigation and Threat Management Records • DEPT-29, Unmanned Aircraft Systems • DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations
	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: Management and Information Systems (N1-040-87-004)
	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 to the schedule. Provide explanation: All files are deleted permanently after 90 days of non-use.

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: In the event the information included in the e-mail sent via Kiteworks-Accellion is about the sender or receiver, information stored in the e-mail may be identified by the e-mail address.
X	Quantity of PII	Provide explanation: A significant amount of information may be stored in the system at any point in time from a diverse group of users across the Department.
X	Data Field Sensitivity	Provide explanation: Although encrypted, the subject, although the subject text should not be sensitive, may imply the type of information contained in the encrypted e-mail sent to the receiver from a user.
X	Context of Use	Provide explanation: Any program office may have a user that will require the transfer of sensitive information (e.g. for auditing purposes, investigative purposes, assessment and evaluation, or human resources purposes for personnel processing and management).
X	Obligation to Protect Confidentiality	Provide explanation: aside from other means of encryption methods, with the diverse user type, it is an obligation for the Department to ensure the information is protected, per the use of the Kiteworks-Accellion information system.
X	Access to and Location of PII	Provide explanation: This information system is now to be used in a cloud solution, as opposed to on-premises, as performed previously.
	Other:	Provide explanation:

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 is the potential for insider threat. There are system administrators who monitor the user logs. There is also the potential for sensitive information to be disclosed in the body of a message, even if the documents shared are encrypted. The entire message, if not selected for full encryption of the message itself, may not be encrypted.

Kiteworks-Accellion authenticates organizational users, but validates user accounts through SSO authentication via NOAA ICAM portal or via ADFS LDAP (Active Directory Federation Services Lightweight Directory Access Protocol). The Kiteworks-Accellion system passes the token to NOAA ICAM system which in turn, based on the Bureau that the user selects, transfers the user to the appropriate IDP for authentication. The Kiteworks-Accellion system passes the token to ADFS LDAP for authentication where the user's email address and password are used to authenticate the user.

All user files uploaded for secure transfer are encrypted and temporarily stored on 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.

Training for system administrators is required, as well as a rules of behavior. Cybersecurity and privacy awareness training is required of all users, to mitigate the possibility of insider threat. Thus, potential threat for privacy is minimized.

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.