

**U.S. Department of Commerce  
Office of the Secretary**



**Privacy Threshold Analysis  
for the  
Kiteworks-Accellion**

## U.S. Department of Commerce Privacy Threshold Analysis

### Office of the Secretary/Kiteworks-Accellion

**Unique Project Identifier:** [TBD]

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system:** *Provide a brief description of the information system.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Kiteworks-Accellion 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-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.

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 and does not have any interconnections with other applications.

*d) The purpose that the system is designed to serve*

The DOC Office of the Chief Information Officer (OCIO) currently provides Accellion Secure File Transfer (SFT) services to the Office of the Secretary (OS) and the various departmental bureaus. The Kiteworks-Accellion SFT is a solution offered to users, in which electronic files can be transferred and managed via Federal Information Processing Standard (FIPS) 140-2 validated encryption methods.

*e) The way the system operates to achieve the purpose*

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

*f) A general description of the type of information collected, maintained, used, or disseminated by the system*

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. Kiteworks-Accellion enables various types of data to be transferred in a secure manner. 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.

*g) Identify individuals who have access to information on the system*

The Kiteworks-Accellion Administrator role is the only individual with access to system configuration information. The Kiteworks-Accellion User role is assigned to users of the system, and each user only has access to file transfer data in his/her account. The Kiteworks-Accellion

Administrator has no access to view Kiteworks-Accellion user account data files for transfer service.

*h) 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.

*i) 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.

**Questionnaire:**

1. Status of the Information System

1a. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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):					

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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

- Yes. This is a new information system.
- Yes. This is an existing information system for which an amended contract is needed.
- No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.
- No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes (*Check all that apply.*)

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

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII.

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Other Federal Government personnel
- Members of the public

No, this IT system does not collect any PII.

*If the answer is "yes" to question 4a, please respond to the following questions.*

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

## CERTIFICATION

  X   The criteria implied by one or more of the questions above **apply** to the Kiteworks-Accellion system and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

       The criteria implied by the questions above **do not apply** to the Kiteworks-Accellion system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p><b>Information System Security Officer or System Owner</b>                  Name: Prabhjot Bajwa                  Office: OS Office of Chief Information Officer                  Phone: 202-748-4252                  Email: <a href="mailto:pbajwa@doc.gov">pbajwa@doc.gov</a></p> <p>Signature: <u>Prabhjot Bajwa</u> Digitally signed by Prabhjot Bajwa                  Date: 2021.12.09 06:07:34 -08'00'</p>	<p><b>Information Technology Security Officer</b>                  Name: Jerome Nash                  Office: OS Office of Chief Information Officer                  Phone: 202-482-5929                  Email: <a href="mailto:jnash@doc.gov">jnash@doc.gov</a></p> <p>Signature: <u>JEROME NASH</u> Digitally signed by JEROME NASH                  Date: 2021.12.09 12:25:22 -05'00'</p>
<p><b>Privacy Act Officer</b>                  Name: Tahira Murphy                  Office: Office of Privacy and Open Government                  Phone: 202-482-8075                  Email: <a href="mailto:tmurphy2@doc.gov">tmurphy2@doc.gov</a></p> <p>Signature: <u>TAHIRA MURPHY</u> Digitally signed by TAHIRA MURPHY                  Date: 2022.02.09 16:45:07 -05'00'</p>	<p><b>Authorizing Official</b>                  Name: Lawrence W. Anderson                  Office: Office of Secretary, Chief Information Officer                  Phone: 202-482-2626                  Email: <a href="mailto:landerson@doc.gov">landerson@doc.gov</a></p> <p>Signature: <u>LAWRENCE ANDERSON</u> Digitally signed by LAWRENCE ANDERSON                  Date: 2021.12.09 15:33:30 -05'00'</p> <p>Date signed: _____</p>
<p><b>Bureau Chief Privacy Officer</b>                  Name: Maria D. Dumas                  Office: Office of Privacy and Open Government                  Phone: 202-482-5153                  Email: <a href="mailto:mdumas@doc.gov">mdumas@doc.gov</a></p> <p>Signature: <u>MARIA STANTON-DUMAS</u> Digitally signed by MARIA STANTON-DUMAS                  Date: 2022.02.10 18:43:22 -05'00'</p>	<p> </p>