Federal Trade Commission
Privacy Impact Assessment

Accellion

(aka Secure File Transfer System (SFTS))

Updated April 2023

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC, Commission or the agency) is an independent federal government law enforcement and regulatory agency with authority to promote consumer protection and competition through prevention of unfair, deceptive and anti-competitive business practices; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish these missions without unduly burdening legitimate business activity.

The Secure File Transfer System (SFTS) uses a commercially available software appliance. This software appliance enables authorized FTC employees and non-FTC users to send and receive copies of files and other electronic data to one another over the Internet. SFTS uses enhanced encryption and authentication methods provided by a managed file transfer process that can be securely accessed through a standard Internet Web browser (e.g., Internet Explorer, Firefox). The main purpose of this system is to allow the electronic exchange of large and/or sensitive documents and other data files between the FTC and outside parties in agency law enforcement investigations, litigation, studies, and events. The SFTS is intended to provide an easy, fast, reliable, and safe alternative to other file shipping or transfer procedures currently in use (e.g., sending and receiving documents or data by courier, private express, or postal service in paper or CD-ROM/DVD format). In particular, for voluminous files or data already in electronic format, SFTS should reduce the considerable time, effort, cost, and risks associated with converting, shipping, receiving, and storing such files or data by more traditional methods. All files uploaded to the SFTS are checked for viruses.

The SFTS is used to collect, maintain, or disseminate documents and files, some of which may include personally identifiable information (PII) about members of the public (e.g., individual defendants, consumers, or others). Accordingly, we have conducted this privacy impact assessment (PIA) and are making it available to the public, as required by section 208 of the E-Government Act of 2002, to explain how the FTC has considered the possible privacy risks of such a system and how we have addressed those risks.

To understand the privacy risks of the SFTS, it is important to understand the four main SFTS user groups: administrators, licensed users, guests, and form users.

The URL for the Kiteworks cloud is: https://ftc.kiteworks.com/

Administrators	Only FTC staff can be administrators. Administrators administer the application and can create users, run reports, perform system updates, and perform other tasks to ensure system functionality and security.
Licensed Users	Only FTC staff can be licensed users of the FTC account. Only licensed users can initiate SFTS transactions. Licensed users can send files, request files, and receive files using the application.
Guests	FTC staff or non-FTC users (including members of the public) can use SFTS as guests. Non-FTC users would only achieve guest status on the FTC SFTS account if an FTC licensed user initiated

	a transaction with them, such as requesting documents from them or sending documents to them. After the FTC-licensed user uses SFTS to send the guest user the appropriate hyperlink to a secure web page, the guest user (and only that guest user) can complete the transaction initiated by the licensed user, such as sending (uploading) requested documents or receiving (downloading) sent documents. The guest user cannot perform other actions within the system aside from the action requested by the FTC-licensed user. For instance, the guest user cannot use SFTS to send files to destinations that were not requested by the FTC-licensed user.
Form Users	Members of the public may input information into web-based forms set up by the FTC that use the SFTS platform. These forms may be used, for instance, to submit information and files for conferences or for law enforcement actions. The content of the forms, and the types of files requested, will depend on the purpose for which the form has been set up.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, the Commission Rules of Practice, and other statutes and regulations enforced by the agency authorizes the FTC to collect the information that is sent, received, and maintained temporarily in the system.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☐ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☐ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: PIN/Password, Any other information (including PII) contained in the content of files being transferred. See explanation under "File/form content" below.
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

SFTS stores two main categories of data: user/administrator data and file/form content.

User/administrator data:

Information stored in the SFTS audit log includes e-mail address, IP address, file name, file size, the time the file was sent, the time the file was downloaded, and other actions within the application.

SFTS also stores the username and PIN/password of FTC SFTS administrators, licensed users, and guest users.

File/form content:

The content of files or forms transferred via SFTS could include any type of PII, as information sent, received or temporarily maintained in SFTS is not restricted

[1] Per OMB Circular A-130, personally identifiable information (PII) means 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.

to a specific category or subset of FTC matters, and may relate to any authorized, official FTC matter, such as an FTC law enforcement investigation, lawsuit, or study. Information sent, received or temporarily maintained in SFTS may also relate to other FTC activities, such as conferences or events. The information is in various electronic formats, including word processing files, spreadsheets, databases, e-mails, images, and video or audio files. It consists of materials that the FTC has previously collected (outside the system) or is collecting (through the system) voluntarily (e.g., access letter or discovery) or through compulsory process (e.g., subpoenas, civil investigatory demands, court orders) from various businesses or individuals (see section 2.2 below). The materials that can be uploaded and downloaded from the system include documents that the FTC staff themselves have compiled or generated (e.g., drafts of joint motions or briefs, attachments, or exhibits, being uploaded and shared with opposing counsel for review). The materials that can be uploaded and downloaded from the system also include documents or information requested from members of the general public.

These documents or files will frequently consist, in whole or part, of nonpublic information, including confidential business data or other privileged or internal matters. In addition, the documents or files may contain personal information about specific defendants, consumers, or other individuals, some of which could raise privacy issues if they were to be improperly handled or disclosed (e.g., personal financial statements, bank records, credit card numbers, customer lists, consumer complaints or affidavits, personal contact data).

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

As noted above, information sent, received or temporarily maintained in SFTS is not restricted to a specific category or subset of FTC matters, and may relate to any authorized, official FTC matter, such as an FTC law enforcement investigation, lawsuit, or study. Information sent, received or temporarily maintained in SFTS may also relate to other FTC activities, such as conferences or events. The information is in various electronic formats, including word processing files, spreadsheets, databases, e-mails, images, video or audio files. It consists of materials that the FTC has previously collected (outside the system) or is collecting (through the system) voluntarily (e.g., access letter or discovery) or through compulsory process (e.g., subpoenas, civil investigatory demands, court orders) from various businesses or individuals (see section 2.2 below). The materials that can be uploaded and downloaded from the system include documents that the FTC staff themselves have compiled or generated (e.g., drafts of joint motions or briefs, attachments, or exhibits, being uploaded and shared with opposing counsel for review). The materials that can be uploaded and downloaded from the system also include documents or information requested from members of the general public.

These documents or files will frequently consist, in whole or part, of nonpublic information, including confidential business data or other privileged or internal matters. In addition, the documents or files may contain personal information about specific

defendants, consumers, or other individuals, some of which could raise privacy issues if they were to be improperly handled or disclosed (e.g., personal financial statements, bank records, credit card numbers, customer lists, consumer complaints or affidavits, personal contact data).

2.3 What is the purpose for collection of the information listed above?

User/administrator data:

SFTS collects user and administrator information to ensure that files and web form information are sent to, and received from, the correct recipients, to ensure that recipients are aware of who has sent the information and vice versa, and to ensure adequate system security and administration.

File/form content:

Files and form information sent or received via the SFTS are used for agency law enforcement or other activities (e.g., studies or special events). As noted earlier, the purpose of the SFTS is to provide a secure alternative to more traditional methods that FTC staff have used to exchange voluminous or sensitive documents and files with outside parties. The SFTS also helps the FTC satisfy the mandate of the Government Paperwork Elimination Act, which requires that Federal agencies, where feasible, offer electronic options for paper-based filing requirements.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
Administrators, Licensed Users, Guests, and Form Users	See section 2.1 above.
Individuals whose data is included in files being transferred	See sections 2.1-2.2 above. Information sent, received or temporarily maintained in SFTS is not restricted to a specific category or subset of FTC matters, and may relate to any authorized, official FTC matter, such as an FTC law enforcement investigation, lawsuit, or study. Therefore, the way in which data was collected from individuals referred to in files sent via SFTS will vary. Sources of documents and files in the system include: investigational targets (businesses and individuals) or their lawyers or other representatives; other companies or organizations not under investigation; consumers or other witnesses or informants; others (e.g., data acquired by the FTC

	from commercial, academic or governmental sources for investigation, litigation, or study purposes); and the FTC staff themselves (e.g., nonpublic drafts or memoranda, briefs, attachments, exhibits authored by FTC attorneys). Materials maintained in the system are not necessarily sent by or received from a source through the SFTS; rather, materials in the system are often obtained from sources outside the system (e.g., third-party companies or individuals or consumers) before being uploaded to the system.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
Members of the public	Members of the public who use SFTS as form users or guests may have access to the data they sent or received. For more information, see the chart under Section 1.1.
FTC Staff and Contractors	FTC staff and contractors authorized to send or receive information via SFTS, or authorized to perform backend maintenance or administration of SFTS, may have access to SFTS data. For more information, see the chart under Section 1.1.

Contractors working for the secure file transfer system vendor do not have access to FTC data.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

FTC contractors use the Secure File Transfer System. FTC contractors are required to sign nondisclosure agreements, complete security and privacy training prior to obtaining access to any systems, and complete annual security and privacy training to maintain network access and access to those systems.

☐ Not Applicable.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

The FTC contractors who use the Secure File Transfer System must follow the reporting and other procedures in the FTC's Breach Notification Response Plan.

☐ Not Applicable.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☐ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☐ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): See below

☐ Notice is not provided (explain): _____

Wherever required, the FTC provides notice to individuals about its policies regarding the use and disclosure of information at the time information is collected (e.g., in voluntary access letters, civil investigatory demands, or agency forms or questionnaires that were originally used to request or collect the information uploaded to the system). SFTS web forms contain an appropriate Privacy Act statement. On those occasions where the FTC cannot provide notice at the time information is collected (e.g. information collected and maintained by other organizations that have then shared such information with the FTC), the FTC provides notice via its privacy policy, its Privacy Act Systems of Records (SORNs), and its PIAs, including this one.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Administrators, Licensed Users, Guest Users, and Form Users	If users choose to use the system, their information will be collected as described in this PIA. However, if prospective users do not wish to have their information collected via SFTS as described in this PIA, they may decline to use SFTS and use other secure file transfer methods instead.
Individuals whose data is included in files being transferred	Yes, in some instances. When information is provided voluntarily to the FTC, the use of such information may also be governed by mutual agreement. If the individual has a right to consent to particular use, this right will normally be exercised when determining whether to provide information to the FTC. However, some uses of information are not

	subject to the consent of the individual providing the information (e.g., information provided pursuant to a court order or subpoena). In addition, uses of information may also be governed by specific laws (e.g., routine uses authorized under the Privacy Act of 1974). Additionally, in some instances, seeking specific consent from all individuals mentioned in files sent via SFTS is likely to pose significant practical hurdles, and in some cases—for instance, when sending files relating to a nonpublic law enforcement investigation—seeking consent from individuals mentioned could also compromise confidential investigations.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted on Data Center GSS. The FTC's privacy policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

The FTC's privacy policy provides links to the FTC's SORNs, which include information about how to correct or amend records. Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov/contact or contact the Chief Privacy Officer directly at cpo@ftc.gov. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners. See also 4.3 above.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Information in SFTS that is used by the FTC as part of its law enforcement, policy, and other activities will be reviewed for accuracy and timeliness in accordance with the specific needs of a particular FTC activity, rather than as part of SFTS. Information in SFTS is also subject to appropriate information security controls, as described elsewhere in this PIA. Appropriate security helps mitigate the risk that SFTS data will be altered via a compromise to the application.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes. Some administrative procedures and technical safeguards are specific to SFTS. For example, for security reasons, internal users of SFTS must register their e-mail address and login to the system (with a password) to upload or download files to or from the system. External guest users of the system must register their e-mail address and log in to the system (with a password) to download files from the system, but are not required to log in to the system (with a password) to upload files to the system following a file request from a FTC SFTS user. External web form users are not necessarily required to input a username/email and password.

Other administrative procedures and technical safeguards apply to many applications and processes at the FTC, including SFTS. For example, all FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OMB guidance. Before any new employee, contractor, or volunteer can access SFTS, that individual must first attend new employee orientation and successfully complete the FTC's Privacy and Security Awareness training.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

The FTC does not routinely use SFTS for system testing, training, or research. However, if the agency is considering whether the SFTS is an effective tool for particular mission activities, the agency may conduct testing on a *de minimis* basis.

☐ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

All files uploaded to the SFTS storage area are deleted from the system once the intended recipient retrieves the files or after a designated time limit, whichever is shorter. Specifically, the file recipient has 96 hours to retrieve the files, but the files are stored on

the server for an additional 24 hours. This disposition conforms with the disposal requirements specified by the National Archives and Records Administration (NARA) in General Records Schedule (GRS) 5.2, item 020, Intermediary Records.

Information collected for the purpose of monitoring SFTS usage, including access, system event, and user logs, and related system technology operations and maintenance records, are retained for three years as specified in NARA GRS 3.1, item 020, Information Technology Operations and Maintenance Records.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

While Accellion may use cookies, it does not share data collected from those cookies with the FTC.

☐ Not Applicable

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Information sent by SFTS could be intercepted in transit over the Internet.	The appliance addresses this risk by using enhanced encryption and authentication methods. Specifically, the SFTS vendor provides three mechanisms for encryption: data-in-transit encryption, data-at-rest encryption, and (optional) file encryption. The vendor uses SSL/TLS 1.2 encryption to secure data in transit between users and SFTS servers. The vendor uses AES-256 to secure data at rest. The vendor uses AES-128 encryption to secure files uploaded and sent through the SFTS. Users decide when to apply file encryption based on the sensitivity level of the file. During training, SFTS users are advised to encrypt files via the SFTS when able, or to use a third-party utility to encrypt the file before it is uploaded. The SFTS's configuration permits information to be transferred only in encrypted form using secure socket layer (SSL) technology, and the user's Web browser verifies the digital signature (i.e., authentication) of the secure Web page where files are uploaded and downloaded.
Files temporarily	To address this risk, when files are not being transferred and

maintained on the system could be improperly accessed by unauthorized individuals or entities.	are at rest in the system, all file names are masked when they are encrypted, which would make it more difficult for a hacker to identify potential file content based on file name. Furthermore, files containing nonpublic information can only be accessed through the URL embedded in the email sent to the appropriate authorized recipient. As noted, files are maintained and available on the system for downloading for only a short period of time before access rights expire and the file is automatically deleted from the system. In addition, the system has a number of security and design controls (including the registration and password-protected login process) that would prevent access to the system if an e-mail invitation is forwarded to a non-recipient, or if the recipient's e-mail box were hacked and a non-recipient obtained access to the invitation e-mail improperly.
Users may inadvertently transfer sensitive data (including sensitive PII) to unintended recipients.	This risk is addressed by a number of administrative (procedural) and technical controls adopted by the FTC or inherent in the software appliance itself. To become authorized to send files via SFTS, FTC employees must receive training, including instructions on how to immediately withdraw (i.e., delete) a file that has been mistakenly uploaded to the system for retrieval by an outside user. There are also specific user guides for internal (FTC) and external (non-FTC) users, explaining the proper use of the system. In addition, to help ensure files are transferred to the correct recipient, the SFTS system is not connected to the user's Outlook address book. Therefore, when users type the address into the "To" field, there is no "auto-complete" unless the user has previously contacted the recipient over the SFTS system. The FTC also asks staff members who have access to the SFTS system to send a test email to verify the recipient's email address and to cut and paste the correct email address from a previous correspondence. Furthermore, all FTC SFTS users must verify that the e-mail address(es) shown in a confirmation box that appears on the user's screen are correct before the invitation e-mail may be sent from the system, and after the e-mail is sent, a "sent mail" confirmation box appears so that the user may verify that the e-mail was sent to the correct recipient.
Users could exceed their authorized access and view documents or files from other accounts.	System administrators do not have access to the files once they are uploaded to the SFTS. Administrators can only view a list of the files being transferred and stored, and can only delete, replicate, and set life cycle rules for each file if necessary. The registration and login process also ensures that user accounts are segregated and that no user has unauthorized access to another user's account. (The system, however, permits users to designate that copies of e-mail invitations be sent to users

	other than the primary recipient, in order to allow shared access to documents and files uploaded to the system, but each user must still register and login to retrieve such files, and cannot gain access to any other files in any other user's accounts.)
A user (whether within the FTC or outside) could upload infected or malicious files and compromise the security of the system.	To address this risk, files uploaded to the SFTS are scanned for viruses, and files found to be infected are rejected. The SFTS anti-virus software receives daily updates to active virus signatures. The FTC recognizes that, despite these precautions, zero-day viruses (defined as a previously unknown virus for which specific anti-virus software signatures are not yet available) remain possible threats.
Once an FTC user downloads documents, files, or other information from the system, there is a risk that it might be improperly stored or maintained, which might make it vulnerable to loss, theft, misuse, etc.	By internal FTC information security policy, FTC users are prohibited from storing any sensitive PII on desktop computers. All such materials, if any, may only be stored on secured network drives with restricted access. There are further restrictions on the handling or further shipping, transfer, use, and destruction of such sensitive materials (e.g., encryption, logging, supervisory approval).
SFTS information could be compromised during the information disposal process.	An overall discussion of the privacy risks associated with the SFTS and the steps that the FTC has taken to mitigate those risks is provided in section 2.8, above. The privacy risk in disposal of information maintained by the system is relatively low, as data are not moved from the system for destruction, but are deleted in the system after 120 hours if they are not retrieved, per section 7.1. If an FTC user uses the system to download documents or files uploaded by an outside user, and then moves or copies the files to a network drive, or prints such files, the FTC user is responsible for adhering to all internal policies and procedures for the proper destruction of such material when no longer in use and authorized for destruction (e.g., nonpublic materials must be properly shredded or burn-bagged).

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

See the first paragraph of section 5.2 above.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Yes, records in the system, to the extent retrieved by personal identifier, are covered by existing SORNs, although the SFTS itself does not maintain a unique system of records retrieved by individual name or other personal identifier under the Privacy Act. Rather, documents and files sent to the FTC through SFTS are normally incorporated into FTC investigatory files. Those investigatory records are described in and covered by the Privacy Act SORN designated as FTC-I-1, Nonpublic Investigational and Other Nonpublic Legal Program Records. Similarly, system user data is covered by the SORN designated as VII-3--Computer System User Identification and Access Records–FTC. These SORNs have been published in the Federal Register and posted on the FTC website (see http://www.ftc.gov/foia/listofpaysystems.shtm). The FTC website list of SORNs includes other types of Privacy Act records that the FTC might potentially be transmitted to outside users through the SFTS (e.g., FTC personnel records), although the FTC does not currently intend to use the system for transmitting documents or files other than those described earlier.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.