Federal Trade Commission
Privacy Impact Assessment

$ F F H O O L R Q

D N SE cure File Transfer
System 6) 7 6

Updated $ S U L O

1 System Overview

1.1 Describe the project's 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. 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 incular, for SFTS

	a transaction with them, such as requesting documents from the FTC 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 cited by the agency authorizes the FTC to

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 a needed.		
☐ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth		☐ Internet Cookie Containing
☐ b (ie- 4303757 Td48 p.1 (P (h)3.7 (1)-4 ((r)-10 i)i)8..9 (ir)-5(e (a-b i)i)8.m)1a-TJ 0.0091 Tc 0.004 Tw -29.909.6		
☐	☐	☐
☐		
☐	☐	☐
☐		
☐	☐	☐
☐		☐
☒		
☐	☐	☒
☐		☐
☐	☐	
☐		☐
☐		
☐		
☐	☐	☒
☐	☐	

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 D (y)22.1 ()20 (d)-10 protte(d)-10 pr(t3(.)-8 (g)12 du (F)-4 (T)suuv

☐ 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.

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

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 events, 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's 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	

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 t 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 unauthorized access.

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 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