Federal Trade Commission
Privacy Impact Assessment

for the:

Secure File Transfer System

June 2011

1 System Overview

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 that 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 by using 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 (up to 50 gigabytes) and/or sensitive documents and other data files between the FTC and outside parties in agency law enforcement investigations, litigation, and studies. 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 at rest or in motion in SFTS are encrypted using the applicable Federal standard issued by the Commerce Department's National Institute of Standards and Technology (NIST), i.e.,Federal Information Processing Standards (FIPS) Publication 140-2 validated cryptographic module. All files uploaded to the SFTS are checked for viruses.

There is no external access to the system except for non-FTC users who receive an e-mail invitation from an authorized FTC SFTS user containing a unique hyperlink directing the recipient to a secure Web page hosted by an FTC server, where the recipient–and only that recipient–can send (upload) files to the system for retrieval by the FTC user, or to receive (download) files that have been uploaded by an FTC user to the system for retrieval. For security reasons, internal and external users of the system must register their e-mail address and login to the system (with a password) to upload or download files to or from the system.

The SFTS will be used to collect, maintain, or disseminate documents and files, some of which may include information in identifiable form (i.e., personally identifiable information or 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 before putting the system online.

2. Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

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. The information is in various electronic formats, including word processing files, spreadsheets, databases, e-mails, images, video or audio files, etc., and consist 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 also 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).

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 are the sources of the information in the system?

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; and 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.

2.3 Why is the information being collected, used, disseminated, or maintained?

Files sent or received via the SFTS are used for agency law enforcement or other activities (e.g., studies). As noted earlier, the FTC's purpose 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. How is the information collected?

Information in the form of electronic files (attachments) is uploaded and downloaded with encryption technology by users utilizing their Web browser and a secure web page after registering and logging into the system. As noted earlier in Section 2.2, information may also be collected from sources outside the system before being uploaded to the system for retrieval.

2.5 How will the information be checked for accuracy and timeliness (currency)?

Files are uploaded to the SFTS's secure storage area "as is" without verifying their accuracy or timeliness. Instead, information that is used by the FTC as part of its law enforcement and other activities is reviewed for accuracy and timeliness as required by, and in the course of, the particular activity. For example, staff performing an investigation based upon a consumer complaint may check the information that is obtained to ensure that it is timely and accurate. In other cases, the individual submitting the information may also be required to certify the accuracy of the information (e.g., witness or financial statements in court cases).

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

Yes. The use of a managed file transfer appliance is a new technology that the FTC has not previously employed. Although this technology requires the transfer of potentially sensitive information, including sensitive information about individuals, over the Internet, the system protects the confidentiality and integrity of such information by using authentication and encrypted transport capabilities, thus protecting the information from interception and unapproved use.

2.7 What law or regulation permits the collection of this information?

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.

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

The FTC has identified several risks that could affect the privacy of individuals whose information may be sent, received or maintained in the system.

First, such information could be intercepted in transit over the Internet. The appliance addresses this risk by using enhanced encryption and authentication methods. 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.

Second, there is the risk that files temporarily maintained on the system could be improperly accessed by unauthorized individuals or entities. To address this risk, when files are not being transferred, and are at rest in the system, all file names are masked when they are encrypted using a FIPS 140-2 validated cryptographic module. 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 expires 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 passworded 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.

Third, there is a risk that 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 an authorized SFTS user, FTC employees must receive classroom or one-on-one 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.

Fourth, to prevent the risks of system users exceeding their authorized access and viewing 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.)

Fifth, there is the risk that 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 (a previously unknown virus for which specific anti-virus software signatures are not yet available) remain possible threats.

Sixth, once an FTC user downloads documents or files 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).

3. Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

As discussed in the introduction and system overview (see Section 1), information in the system may be used to support the FTC's law enforcement and other activities, including to investigate and enforce statutes and regulations protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace; to locate victims; to assist with redress; to investigate internal matters; and to defend against suits brought against the agency.

3.2 Which internal entities will have access to the information?

Only FTC employees (and authorized FTC contractors) who have received either classroom or one-on-one training on the proper use of the system are granted permission to use SFTS internally at the FTC. User IDs can only be created by a System Administrator, and access will remain in place until there is no longer a business need or when the employee leaves the agency. The system owner for SFTS is the Information Assurance Branch in the Office of the Chief Information Officer.

3.3 Which external entities will have access to the information?

An external party will not have access to the SFTS unless that party receives an invitation from an authorized FTC SFTS user. Only after receiving an invitation from an FTC SFTS user, can an external party can send files to the SFTS for pick up by an FTC user. As noted earlier, external users are, in addition, required to register and login with a password to use the system.

4. Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

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). For SFTS users, appropriate notice is given at the secure Web page where their user login information is collected. 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.

5. Web Site Privacy Issues

5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).

HTTPS/SSL is used for user authentication and file transport purposes. There are temporary session cookies associated with these activities. As noted earlier, the user must also register (with e-mail address) and provide his or her user ID (e-mail address) and login (with a password) to use the system, and this data may be stored by the user's computer for future sessions, unless the user checks the on-screen box that states, "I am on a public computer."

6. Security of Information in the System

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements, ensuring the SFTS is appropriately secured. The SFTS resides on the Infrastructure General Support System (GSS) which is categorized as moderate using FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

The SFTS resides on the FTC's Infrastructure GSS, for which a Certification and Accreditation (C&A) has been performed.

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed on the Infrastructure GSS as part of the C&A.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

Yes. However, as discussed in section 2.8, this technology uses several layers of authentication to ensure that only authorized recipients can access the files and encryption of the files in motion and at rest. In addition, the system utilizes various administrative and technical controls to address various other privacy risks identified and discussed earlier. Accordingly, the privacy risks of the technology are considered low in terms of confidentiality, integrity, and availability.

6.5 What procedures are in place to determine which users may access the system and are they documented?

All FTC employees using this system must be pre-approved by their supervisor and receive class room or one-on-one training on the appropriate use of this technology. In addition, all users must read and sign a rules of behavior, acknowledging their responsibilities while using the SFTS. Non-FTC users are authorized by invitation only and must comply with a registration and login that prevents access to the system and the user's account by unauthorized persons or entities.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC staff approved to use the SFTS are required to complete computer security and privacy awareness training annually. Interactive online training covers topics such as properly handling of sensitive PII and other data, online threats, social engineering, and the physical security of documents. Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities. In addition, as noted above, there is SFTS-specific training for FTC users.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

The SFTS system will track when someone sends a file through the system, from whom the file is sent, to whom the file is sent, and the name of the file. Similarly, the system will track when a file is received, from whom a file is received, the file name, and the IP address of the system onto which the file is downloaded. There is also a documented list of users that have authorized

access to the SFTS system and a comprehensive log that can be filtered to look for file withdrawals, successful logins, failed logins, and file activity.

6.8 Questions regarding the security of the system.

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7. Data Retention

7.1 For what period of time will data collected by this system be maintained?

All files uploaded to the SFTS storage area are deleted from the system once the intended recipient retrieves the files or after 72 hours, whichever is shorter. Therefore, the SFTS never maintains files for longer than 72 hours. Uploaded files are not copied to any type of storage media during the normal course of operations.

Information collected for the purpose of monitoring SFTS usage, including access, system event, and device usage logs, will be deleted or destroyed when the FTC determines it is no longer needed for audit purposes.

7.2 What are the plans for destruction or disposal of the information?

Information is retained and destroyed in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA), and any applicable technical security standards issued by NIST. The FTC has submitted to NARA a comprehensive records disposition schedule, SF-115 Request for Disposition Authority. Pending NARA approval, FTC will manage usage information in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 C.F.R. Ch. XII, Subchapter B, Records Management, and the Office of Management and Budget (OMB) Circular A-130, par. 8a1(j) and (k) and 8a4.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

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 72 hours if they are not retrieved. 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. Privacy Act

8.1 Will the data in the system be retrieved by a personal identifier?

Documents or files maintained in the system are not retrieved in the system by a personal identifier (e.g,. name or other personally assigned number or identifier). The system, however, does maintain user accounts, including login passwords, that may be retrieved according to unique user ID (e.g., e-mail address) by a system administrator.

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

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 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's Web site (see http://www.ftc.gov/foia/listofpaysystems.shtm). The FTC's Web site 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.

9. Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of information in this system is consistent with the FTC's Privacy Policy.

10. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____

Jack Gabriel
IT Security Specialist

Review:

_____ Date: _____

Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____

Marc Groman
Chief Privacy Officer

_____ Date: _____

Margaret Mech
Information Assurance Manager

_____ Date: _____

Jeffrey Nakrin
Director, Records and Filings Office

Approved:

_____ Date:_____

Jeffrey Huskey
Chief Information Officer