Federal Trade Commission
Privacy Impact Assessment

for the:

E-Filing System

Updated May 2015

1. System Overview

The E-Filing System is a web-based application that the Federal Trade Commission uses to receive public and nonpublic filings in adjudicative proceedings conducted under Part 3 of the Commission's Rules of Practice, 16 C.F.R. pt. 3. These filings are submitted by FTC staff acting as complaint counsel, outside attorneys representing respondents, and third-party participants ("parties").

When the E-Filing System was first launched, parties in these proceedings filed their nonpublic motions, memoranda, briefs, exhibits and other submissions in paper form, and their public motions, memoranda, briefs, exhibits and other submissions via the FTC's E-Filing System. In May 2015, the Commission deployed enhancements to the E-Filing System to enable parties to file nonpublic documents through the System as well.

All Part 3 filings, except for confidential portions, are treated as part of the agency's public record, and are routinely made available to the public. See Commission Rule 4.9(b), 16 C.F.R. § 4.9(b). Public Part 3 filings, with the exception of very lengthy attachments, are posted on the FTC's public website, FTC.gov.

The E-Filing System reduces the time, expense, and burden associated with filing, while continuing to ensure the security, integrity and availability of such filings by enabling parties to use a secure website to submit public and nonpublic filings electronically over the Internet. The E-Filing System also implements the Government Paperwork Elimination Act, which requires that agencies, when practicable, offer electronic alternatives for agency filing requirements. *See* Pub. L. No. 105-277, tit. XVII, § 1704(1), 112 Stat. 2681, 2681-750 (Oct. 21, 1998).

The E-Filing System (System) is operated by a contractor on behalf of the FTC. The System comprises the following components:

- Register for E-Filing - enables parties to register to use the System;
- Submit a Notice of Appearance - a required web form that is completed by a party to participate and submit documents in a particular proceeding;
- Submit an E-Filing - allows registered parties to e-file a document in the E-Filing System; and
- Docket Sheet - allows Attorneys of Record on the Notice of Appearance (i.e., complaint counsel and counsel for respondents) and authorized FTC staff and contractors in the Records and Filings Office (RFO), and authorized staff in the Office of the Secretary (OS) and Office of Administrative Law Judges (OALJ) to view the history and status of filings.

The titles of all public and nonpublic filings submitted in a particular matter are listed on the Docket Sheet. Public filings will contain a link to the document. Nonpublic documents that have been submitted into the E-Filing System are only accessible by authorized RFO staff and contractors and authorized OS and OALJ staff. In addition, the E-Filing System includes other components that are designed for RFO staff and contractors to process and review the filings and to export public filings for posting on the FTC.gov website.

Through the E-Filing System, parties (including third-party participants) may also provide electronic service of public filings, rather than paper service, to Attorneys of Record (i.e., complaint counsel and counsel for respondents) who have opted-in for electronic service. Third-party participants (unlike Attorneys of Record) cannot receive service through the System. When electronic service is provided through the E-Filing System, the System will generate an email to the Attorneys of Record being served that includes a link to the submitted document in the Docket Sheet. The filer will have the option of appending a Notice of Electronic Service PDF to the end of the document if the filer serves the document electronically. The Notice of Electronic Service, similar to the certificate of service, provides a listing of who was served via the E-Filing System as well as others served outside the System.

The System Owner for the FTC's E-Filing System is RFO, which is located in the FTC's Office of the Executive Director.

2. Information Collected and Stored within the System

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

The following information is collected, used, disseminated, or maintained by the System:

Filings. Public and nonpublic filings, including motions, memoranda, briefs, exhibits, notices of appearance, and other submissions from parties to FTC Part 3 adjudicative proceedings. These documents may contain the names, addresses, email addresses, and/or telephone numbers of individuals, including parties to the proceedings as well as witnesses and consumers.

Registration information. Filers are required to register and provide the following registration information: first name; last name; title (optional); name of law firm or employer, if applicable; phone number; fax number (optional); and e-mail address. Filers also specify a login user name and password that will be maintained in the System as part of their registration data. A set of "password recovery" questions are required for the sole purpose of recovering forgotten passwords. The questions chosen and answers provided by the filer also will be maintained by the System.

RFO staff, RFO contractors, Office of the Secretary, Office of the Administrative Law Judge, and vendor staff information. The System collects first name, last name, a login user name and password, work phone number, email address, and password recovery questions and answers chosen by the staff member or contractor. FTC staff and contractors authorized to use the System are required to sign internal Rules of Behavior.

Metadata. The System collects additional information that is maintained and associated with each individual filing (i.e., "metadata"). This includes the filer's System user name, the name(s) of the party or parties on whose behalf the filing is submitted, a filer-defined document title, a document type (from a preset list), and whether the document contains "physical" exhibits. The System also collects the

name and docket number of each Part 3 adjudicative proceeding.

Review information. The System collects certain review information on each document filed. This information includes the receipt date, the document status (e.g., pending, filed (accepted), returned (rejected) and web posted) and any other additional comments from the reviewer (e.g., the reason a document was rejected).

Log data. In addition, the System collects web log data, including IP addresses and date and time information.

Nonpublic filings. Nonpublic filings entered into the E-Filing System contain confidential business information and, potentially, other nonpublic information, including PII.

2.2. What are the sources of the information in the System?

Filings are submitted by registered users of the System ("registrants"). In most instances, these filings are submitted directly to the System by the registrants; in others, RFO staff scan and upload documents into the System when the documents have been filed in paper form. The source of personal information contained in a document is the individuals to whom the document pertains to or, in some instances, from other individuals, such as employees of respondents in a Part 3 matter, and consumers who may have done business with respondents. Nonpublic information (in nonpublic filings) may come from respondents, third parties, and others, such as employees of respondents.

Registration information and metadata is provided by the registrants themselves (except that RFO staff and contractors provide the name and docket number of each Part 3 adjudicative proceeding). Registrants include FTC complaint counsel, counsel for respondents, and any other users who will be submitting filings through the System.

RFO staff, RFO contractors, Office of the Secretary, Office of the Administrative Law Judge, and vendor staff information is provided by the individual staff member or contractor.

Review information is entered by the System automatically (e.g., receipt date) or by RFO staff and contractors (e.g., that a document has been accepted).

Log data is generated and maintained automatically by the System.

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

The purpose of the E-Filing System is to facilitate the submission, tracking and management of public and nonpublic filings via electronic means, including electronic service of public filings, and web posting of such filings in Part 3 adjudicative proceedings.
Registration information and RFO staff, RFO contractors, Office of the Secretary,

Office of the Administrative Law Judge, and vendor staff information is collected for system administration and security (e.g., password recovery) purposes.

Review information is used by RFO staff and contractors, and OS and OALJ staff to determine the status of a document.

Log data is collected for audit and System security purposes (e.g., to help detect unauthorized access or intrusion and report, use, or refer such information as necessary for further investigation or other action).

2.4. How is the information collected?

With the exception of log data and document receipt date, all information in the E-Filing System is collected via a web-based form. All users, including registered users and FTC staff, enter or upload the information directly into the web-based form.

Log data is generated by the System automatically.

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

Filers are responsible for submitting accurate information and for updating it as appropriate during the proceeding.

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?

No. For discussion of how use of the technology affects individuals' privacy, see Sections 2.8 and 4.5.

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

The FTC Act, the Commission's Rules of Practice, and other laws and regulations that the Commission enforces permit the collection of the information. For more information, see https://www.ftc.gov/enforcement/statutes.

The Federal Information Security Management Act (FISMA) and other information security laws authorize the FTC to collect user and log data for IT audit and security purposes.

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

Two main privacy risks have been identified.

The first risk is that a public document filed via the E-Filing System, and placed on

FTC.gov, could contain sensitive personal information, such as Social Security Numbers. The risk that documents will contain sensitive personal information is mitigated by clear instructions and warnings to users that the public filings will become part of the Commission's public records and will be posted on FTC's publicly accessible website, FTC.gov.

The System provides specific instructions that each public document filed must be clearly marked "PUBLIC DOCUMENT" and must not contain any *in camera* or other confidential information. The Commission's Rules of Practice prohibit the inclusion of sensitive personal information in a public filing. It is the responsibility of the filer, and not the Federal Trade Commission, to ensure that the document is properly marked, that it contains no confidential or sensitive personal information, and that all redactions are complete, permanent, and irreversible.

Prior to submission of any public documents, the user is required to respond, on a document-by-document basis, to the question, "Does this document contain nonpublic information?" If the user answers "yes" for any document, the System displays a message that the document cannot be submitted under the public filings section of the E-Filing System. Prior to submission of a public document, users must also affirmatively acknowledge that they have followed the filing instructions, including the prohibition on filing any nonpublic materials under the public filings section of the System.

The second risk identified is that information in the E-Filing System, including nonpublic filings, will be viewed or altered by unauthorized parties. This risk is mitigated in several ways. The System utilizes encryption technology in the transmission of data across the Internet (HTTPS/SSL), while data is at rest, and for login security, to encrypt passwords in the database. All users are required to login with a user name and password, based on the FTC's strong password requirements.

To help reduce the risk of alteration, filings submitted through the E-Filing System are filed in Adobe Portable Document Format (pdf), which cannot be altered as easily as standard word processing documents. Access to documents in the System is granted only to authorized RFO staff and contractors for processing, review and administration, on a read-only basis to authorized OS and OALJ staff and, for public documents only, on a read-only basis to Attorneys of Record (i.e., complaint counsel and counsel for respondents).

Because authorized RFO staff and contractors (including the vendor's staff) and OS and OALJ staff can access nonpublic filings in the System, they are required to use multi-factor authentication to log in to the System. In contrast, no Attorneys of Record (i.e., complaint counsel and counsel for respondent) or third-party participants may access nonpublic filings in the System. This is true even for the Attorneys of Record that file nonpublic documents; once such documents are submitted to the System, only RFO staff and contractors, OS staff and OALJ staff can view the documents.

Further, as noted earlier, third-party participants may not receive service through the

System of any filings, including public filings, and may not even access such filings through the System. (Such participants may view such filings only when posted on the public FTC website.) In addition, FTC staff and contractors and subcontractors are subject to security background checks.

3. Use and Access to Data in the System

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

The purpose of the E-Filing System is to facilitate the submission of public and nonpublic filings via electronic means, electronic service of public filings, and web posting of public filings in Part 3 adjudicative proceedings.

Filings initially will only be viewable by authorized FTC staff and contractors and, for public filings in a Part 3 proceeding, by Attorneys of Record (i.e., complaint counsel and counsel for respondents) who have registered with the System and submitted a Notice of Appearance in the proceeding. Once a public document, including the relevant metadata, is designated as "filed" (accepted), it will become part of the public record and be posted to the public website at FTC.gov. With the exception of date stamping, these documents are provided to the public exactly as received. Nonpublic documents can only be viewed in the System by authorized FTC staff and contractors. The titles of nonpublic documents can be viewed by Attorneys of Record in the proceeding in the Docket Sheet for the proceeding, but Attorneys of Record cannot view the underlying nonpublic document(s) once the document(s) have been submitted to the System.

Registration information and metadata are used to ensure that only authorized individuals have access to and submit filings to the System.

Review information is used by RFO staff and contractors and OS and OALJ staff to determine the status of a document.

Administrative data is used for System administration and security purposes (e.g., password recovery).

Log data is used for System audit and security purposes.

3.2. Which internal entities will have access to the information?

FTC staff who serve as complaint counsel, have registered with the System, and have submitted a Notice of Appearance in a particular matter will have the ability to review and modify their documents in the System prior to submitting them. Filers, including FTC complaint counsel, cannot use the System to edit their submitted documents. Complaint counsel who have registered with the System and submitted a Notice of Appearance in a proceeding can access the Docket Sheet for the proceeding on a read-only basis, including public documents that have been submitted, "filed"

(accepted) and "returned" (rejected) as well as the titles of nonpublic documents that have been submitted, filed or returned. Once the public documents are posted, they can be accessed on the FTC's website, FTC.gov. As noted earlier, complaint counsel may not access and retrieve any nonpublic filings from the System (including their own filings).

Authorized RFO staff and contractors will have access to information for processing, review and administration (e.g., adding a new user account or proceeding) purposes. Read-only access will be available to authorized OS and OALJ staff.

3.3. Which external entities will have access to the information?

External filers (e.g., counsel for respondents) who have registered with the System and have submitted a Notice of Appearance in a particular matter will have the ability to review and modify their documents in the System prior to submitting them. Filers cannot use the System to edit their submitted documents. Counsel for respondents can access the Docket Sheet for the proceeding on a read-only basis, including public documents that have been submitted, "filed" (accepted) and "returned" (rejected) as well as the titles of nonpublic documents that have been submitted, filed or returned. Once the public documents are posted, they can be accessed on the FTC's website, FTC.gov. As noted earlier, external filers may not access and retrieve any nonpublic filings from the System (including their own filings).

The System is maintained and operated on behalf of the FTC by a contractor. The System administrator has full access rights to all documents and metadata in the System in order to assist with maintenance of and enhancements to support the System's operations (the System administrator cannot alter any document that has been submitted into the System).

Registration information and information about a particular transaction (e.g., any error messages the filer may have received) will be available to FTC contractors in order to provide help desk support and to maintain the operations of the System. This access will be read-only, except for passwords and user IDs that they may have to reset as part of their support and maintenance of the System.

Information collected by the E-filing System for administrative purposes (e.g., registration information) is not provided to the public via 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?

The System utilizes web forms to ask the user for the information and provide notice about what information is collected, and how it is used and disclosed.

4.2. Do individuals have the opportunity and/or right to decline to provide information?

Yes. If the individual does not want to provide information through the System, then, under the Commission's Rules of Practice, the individual may file documents in paper form.

4.3. Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Individuals do not have the right to consent to particular uses of the information stored in the System except by declining to provide the information.

4.4. What are the procedures that allow individuals to gain access to their own information?

See Sections 3.2 and 3.3. Internal and external filers can also access their nonpublic registration information via the System. Individuals may also file a Privacy Act request to gain access to their own information.

4.5. Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

The privacy risk identified is that information in the System will be viewed or altered by unauthorized parties. See Section 2.8 regarding how this risk has been mitigated.

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).

The System uses a session cookie to store authentication information. This cookie is deleted when the browser is closed or when the user logs out of the System.

The System does *not* use persistent cookies, web beacons, or other persistent tracking technology.

5.2. If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

The System utilizes encryption technology in the transmission of data across the Internet (HTTPS/SSL), while data is at rest, and for login security so passwords are encrypted in the database.

Every page of the web site will contain a link to the FTC Privacy Policy.

5.3. Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

See Section 2.8.

5.4. If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

The System does not collect, use or disclose personal information obtained from children under 13 nor is it directed at children.

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?

Yes. All IT security requirements and procedures required by federal law are being followed to ensure that information is properly secured.

6.2. Has an Assessment and Authorization been completed for the System or Systems supporting the program?

Yes. An Assessment and Authorization has been completed.

6.3. Has a risk assessment been conducted on the System?

Yes. A security risk assessment has been performed on the System.

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

The System uses web-based forms, but precautions have been taken to ensure the security of such forms as described elsewhere in the PIA. See Sections 2.6 and 2.8.

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

A filer must complete the registration process and file a Notice of Appearance for a specific active proceeding to file documents in that proceeding. RFO has procedures in place to grant access to RFO staff and on-site contractors who will review and process submitted documents, and read-only access for OS and OALJ staff. Access is granted to individuals only if needed to perform their work. The vendor also has procedures in place to grant System access to vendor's staff. Access is only granted to the vendor's staff if needed to perform their work.

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

All FTC staff and all contractors with network access receive privacy training on an annual basis. Relevant staff and contractors in RFO receive specific training on the use of the E-Filing System. All vendor staff with access to the System receive both FTC privacy training and the vendor's own privacy training on an annual basis.

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

The System is categorized based on Federal Information Processing Standards (FIPS) security categorization and on the National Institute of Standards and Technology (NIST) Security Control guidance as a moderate risk System.

Because the System contains nonpublic documents, individuals (e.g., RFO and OALJ staff) with access to those documents use multi-factor authentication to log into the System. See Section 2.8. Attorneys of Record do not have access to such nonpublic documents and are permitted to log into the System using single-factor authentication. The E-Filing System has been designed to prevent all unauthorized access to the data contained in the System, including unauthorized access by administrators and developers. The System has undergone a certification process to validate the integrity of the access controls. The access controls comply with the Security Technical Implementation Guide (STIG) that NIST guidance sets out for a moderate risk System. The application's access controls include regular auditing and testing of the System.

6.8. To whom should questions regarding the security of the System be directed?

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 public and nonpublic filings submitted via the E-Filing System are maintained as received (i.e., the original information is not overwritten) and will be retained in the E-Filing System until there is no longer a business need. The FTC prints the public and nonpublic filings from the E-Filing System and includes the printouts with the Administrative Record of the proceeding, which is maintained in hard copy. The Administrative Record will be retained in accordance with the FTC NARA-approved disposition schedule, N1-122-09-1.

The E-Filing System web forms and metadata will be retained in accordance with the FTC NARA-approved disposition schedule. Registration information, RFO staff,

RFO contractors, Office of the Secretary, Office of the Administrative Law Judge, and vendor staff information, and log data will be retained in accordance with General Records Schedule (GRS) Transmittal 23, GRS 3.0 (technology records) issued by NARA.

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

All E-Filing information will be deleted/destroyed in accordance with OMB, NARA, and NIST regulations and guidelines.

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

See Section 2.8 regarding risks identified in the data retention and how they have been mitigated. All E-Filing information will be deleted/destroyed in accordance with OMB, NARA, and NIST regulations and guidelines.

8. Privacy Act

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

Yes. Information filed by users is tied to a user account, which is identified by a user-defined user name and password. The search feature in the Docket Sheet enables retrieval of data by personal identifier (e.g., an individual's name) in document titles but does not enable searches within the documents themselves. Authorized FTC staff and contractors who have access to nonpublic documents are required to use a multi-factor authentication solution that requires a personal identifier in addition to their name, user name and password. Likewise, the System maintains log or other administrative data that may be retrieved by user name.

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

Public filings received through the System are covered by FTC I-6. Nonpublic filings received through the System are covered by FTC I-1. System user data are covered by FTC VII-3. See https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems (system of records notices).

9. Privacy Policy

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

The collection, use, and disclosure of information in the System have been reviewed to ensure consistency with the FTC's privacy policy posted on the FTC's website, www.ftc.gov.

10. Approval and Signature Page

Prepared by:

_____ Date: _____
Jeffrey D. Nakrin
Director, Records and Filings Office

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Katherine Race Brin
Acting Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

Approved:

_____ Date: _____
Pat Bak
Acting Chief Information Officer