Federal Trade Commission
Privacy Impact Assessment

FTC E-Filing System
(E-Filing)

Updated April 2018

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The E-Filing system is a web-based application that allows participants to electronically file public and nonpublic documents in the Federal Trade Commission's 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, third-party participants, the Administrative Law Judge, and the Office of the Secretary ("parties").

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.[1] 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.[2]

The E-Filing system is part of a larger vendor-operated system known as CommentWorks.[3] CommentWorks is managed by a contractor, ICF Technologies, on behalf of the FTC. The system comprises the following components:

- Register for E-Filing - enables parties to register to use the system. During the registration process, the system collects the registrant's full name; company name; work address; work telephone number; facsimile number; email address; User ID; and PIN/Password;
- Submit a Notice of Appearance - a required web form that is completed by a party to participate and submit documents in a particular proceeding. The Notice of Appearance form collects the parties' full name; State Bar Association Number; company name; work address; work telephone number; facsimile number; email address; the name of the represented company; and the represented company's address;
- 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), authorized FTC staff and contractors in the Records and Information Management (RIM) Office, 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 contain a link to the document. Nonpublic documents that have been submitted into the E-Filing system are only accessible to authorized RIM staff and contractors and authorized Office of the Secretary (OS) and Office of the Administrative Law Judge (OALJ) staff. In addition, the E-Filing system includes other components that are designed for RIM staff and contractors to process and review the filings and to export public filings for posting on the FTC.gov website.

[1] *See* Commission Rule 4.9(b), 16 C.F.R. § 4.9(b).
[2] *See* Pub. L. No. 105-277, tit. XVII, § 1704(1), 112 Stat. 2681, 2681-750 (Oct. 21, 1998).
[3] For more information about this system, see CommentWorks PIA.

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 documents through the E-Filing 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. Individuals cannot access any filings through the E-Filing system itself; they have only limited, read-only access to system docket sheets showing the history and status of their filings. The filer has 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 FTC system owner for the E-Filing system is RIM, which is located in the FTC's Office of the Chief Administrative Service Officer (OCASO).

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

The E-Filing system implements the Government Paperwork Elimination Act, which requires that agencies, when practicable, offer electronic alternatives for agency filing requirements.[4]

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 Modernization Act (FISMA) and other information security laws authorize the FTC to collect user and log data for IT audit and security purposes.

[4] *See* Pub. L. No. 105-277, tit. XVII, § 1704(1), 112 Stat. 2681, 2681-750 (Oct. 21, 1998).

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[5] 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)*:State Bar Association Numbers; see additional details below
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☒ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

Filings. Public and nonpublic filings include 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 are maintained in the system as part of their registration data.

RIM staff and contractors, OS, OALJ, and vendor staff information. The system collects first name, last name, a login user name and password, work phone number, and email address.

Metadata. The system collects additional information that is maintained and associated with each individual filing (i.e., "metadata"). This includes the filer's 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.

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

[5] 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.

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

Parties must also certify that they are in good standing with their state bar association and provide their bar number.

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.

Registration information. Filers are required to choose a set of "password recovery" questions for the sole purpose of recovering forgotten passwords. The questions chosen and answers provided by the filer are also maintained by the system.

Review information. The E-Filing 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).

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

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

Review information is used by RIM 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 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***
Participants in FTC's Part 3 Administrative Proceedings	In FTC adjudicative proceedings, participants that choose to submit electronic filings must do so via the web-based E-Filing system. Participants are asked to provide registration information, such as first name; last name; title (optional); name of law firm or employer, if applicable; phone number; fax number (optional); and e-mail

Source of Data	*Type of Data Provided & How It Is Collected*
	address. Filers also specify a login user name and password that is 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. Participants also upload filings pursuant to the case. All filings are collected via web submissions through the E-Filing system and maintained in the FTC's Electronic Document Management system (Documentum).[6]
FTC personnel	Authorized RIM staff, OS staff, and OALJ staff are granted access through a separate registration process. During system registration, authorized staff are asked to provide registration information, such as first name; last name; name of organization; phone number; and e-mail address. Authorized staff 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.
E-Filing System	Review information is automatically entered by the E-Filing system itself (e.g. receipt date). Log data is generated and maintained automatically by 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*
FTC Staff and Contractors	Authorized RIM 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. FTC staff serving as complaint counsel, who have registered with the system, and who 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 submission. Complaint counsel who have registered with the system and submitted a Notice of Appearance in a proceeding can access the Docket Sheet and view public documents for the related 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. Complaint counsel may not access and retrieve any nonpublic filings from the system (including their own filings).

[6] *See* Documentum PIA for more information on this system.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
External Participants	External parties serving as respondents' counsel or counsel for third parties, who have registered with the E-Filing 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 submission. Respondents' counsel who have registered with the E-Filing system and submitted a Notice of Appearance in a proceeding can access the Docket Sheet and view public documents for the related 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. Third Party counsel cannot access the Docket Sheet nor can they view any documents in the system. External parties may not access and retrieve any nonpublic filings from the system (including their own filings).
ICF Technologies	The E-Filing system is maintained and operated on behalf of the FTC by ICF Technologies. The ICF system administrator has full access rights to all documents and metadata in the E-Filing 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 IT 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.

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.

The E-Filing system is part of a larger vendor-managed system called CommentWorks. CommentWorks is maintained and operated by ICF on behalf of the FTC. The CommentWorks system administrator has full access rights to all documents and metadata in the E-Filing system in order to assist with maintenance of and enhancements to support the E-Filing system's operations (the system administrator cannot alter any document that has been submitted into the system). As part of ICF's mandatory annual security training, all ICF staff are required to complete data privacy training that emphasizes the importance of safeguarding personal data handled or maintained by ICF staff in the course of supporting its clients. Additionally, ICF's Project Manager and System Security Officer participate in the FTC's annual Privacy and Security Awareness Training.

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 FTC Help Desk technicians may have to reset as part of their support and maintenance of the system.

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.

ICF maintains incident response procedures that are implemented by its Corporate IT Information Security (CIT InfoSec) Team. These procedures are applied to incidents arising with ICF-owned systems as well as customer-hosted systems that do not have their own specified incident response protocols. The FTC systems hosted by ICF are subject to government-wide policies on breach notification and response. Thus, ICF has prepared an FTC-specific set of incident response procedures that apply to the CommentWorks system regarding notification timelines, a reporting matrix, roles and responsibilities, emergency communication procedures and up-to-date contact information.

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: FTC's Privacy Act Statement is located on the homepage and on the login page of the system. The Statement explains: (1) the legal authority for the system; (2) the system's purpose; (3) the ways the information collected by the system may be routinely used or disclosed outside the agency ("routine uses"); and (4) whether the system is voluntary or mandatory, including the legal or other effects on the individual if the system is not completed. The "Privacy Act statement" is intended to help individuals make informed decisions about whether to provide the information requested by the system.
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain): _____

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)?

Yes, an individual can choose not to provide data about themselves for the E-Filing system by not registering with the system. If they choose not to register, then they will not be able to use the E-Filing system to electronically file. Under the Commission's Rules of Practice, individuals may file documents in paper form instead. However, if they fail to provide the necessary information (in paper form) as part of their filing, they may be denied participation in the FTC's Part 3 Administration proceedings. Pursuant to Commission Rule 4.1(d), 16 C.F.R § 4.1(d), parties who

wish to appear before the Commission or an Administrative Law Judge are required to submit a Notice of Appearance.

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

Individuals may access their personally identifiable information provided during the registration process by logging into the E-Filing system and reviewing and updating their account information as necessary. However, if there is a change to individual's employer, he/she must notify the FTC and request the old account be closed before registering for a new account under his/her new employer or organization. Pursuant to FTC's Rule 4.9(b), 16 C.F.R. § 4.9(b), the information provided on the Notice of Appearance can be accessed on FTC's website.

Additionally, an individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the E-Filing system. 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 and on the FTC's website. 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.

Yes, see 4.3 above. If incorrect information or outdated information is entered on a Notice of Appearance, the individual can submit a request to RIM requesting that the erroneous/outdated information be removed. The individual must also provide an amended Notice of Appearance.

As specified above in Section 4.3, the FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the agency. The FTC's privacy policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the FOIA and Privacy Act for access to information maintained by the FTC about themselves in the E-Filing system. Such access, and the individual's right under the Privacy Act to make corrections, may be subject to exemptions, as applicable.[7] Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

[7] See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13(m) (FTC Privacy Act rules).

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?

To help ensure the integrity, relevancy, and accuracy of electronic filings and other system data, a filer must complete the registration process and file a Notice of Appearance for a specific active proceeding in order to file documents electronically in that proceeding. As noted earlier, external filing parties (respondent's counsel, third parties) do not have the ability to access any filings (including their own) through the system, to minimize the risk of unauthorized access or exfiltration of confidential, nonpublic material from the system.

Filers are primarily responsible for ensuring that their filing is accurate, complete, and up-to-date. Nonetheless, before accepting a filing, RIM staff review the material and check for its completeness. Once the document has been reviewed and cleared, it is uploaded into FTC's document management system (Documentum) and a paper copy is stored with RIM.. Subsequent updates to materials are submitted through amendments and uploaded, as such, unless specified by the Office of the Secretary. FTC's business functions are not impacted if the data is incomplete. Incomplete data will be returned to the filer and marked as "rejected" or "returned" with an explanation. As noted, filers are responsible for submitting accurate information and for updating it as necessary during the proceeding.

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.

Because the E-Filing system contains nonpublic documents, individuals (e.g., RIM and OALJ staff) with access to those documents use multi-factor authentication to log into the system. 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 an assessment and authorization 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.

RIM has additional procedures in place to grant access to RIM staff and on-site contractors who will review and process submitted documents. Read-only access for OS and OALJ staff is granted to such individuals only if needed to perform their work. ICF also has procedures in place to grant system access to its staff; access is only granted to authorized individuals when needed to perform their assigned work under their FTC contract.

All FTC staff and all contractors with network access receive privacy training on an annual basis. Relevant staff and contractors in RIM receive specific training on the use of the E-Filing system. All ICF staff with access to the FTC's network receive both FTC's Annual Privacy and Security Awareness Training as well as ICF own privacy training on an annual basis.

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

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes. A security risk assessment has been conducted on the system, and the system has received authority to operate.

5.4 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?

☒ Not Applicable. PII is not used in the course of system testing, training, or research.

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 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 in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.2, item 020, Intermediary Records, until there is no longer an agency business need to maintain the documents in the E-Filing system. The Administrative Record will be retained in accordance with the FTC NARA-approved records disposition schedule, N1-122-09-1, schedule 2, Mission Records.

The E-Filing system access records, including access logs and user profiles, will be retained in accordance with NARA GRS 3.2, item 030, System Access Records. Data administration records, such as themetadata from each individual filing, will be retained in accordance with NARA GRS 5.2, item 020, Intermediary Records. .

The system has been configured to record the date PII is collected as well as when PII is deleted. The system will automatically deleted PII 45 days after the FTC determined the case to be closed, and there is no longer a business need to maintain the information.

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.

Yes, the E-Filing system employs the use of a website. The system uses a session cookie to store login/user sessions. No PII is written to the cookie. 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.

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***
A public document filed via the E-Filing system, and placed on FTC.gov, could contain sensitive personal information, such as Social Security Numbers	Clear instructions and warnings are provided 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. In addition, a document submitted that contains sensitive personal information will be treated by the FTC as nonpublic and returned to the filer for redaction and resubmission.
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	A system log is maintained that reflects who accessed the data at any given time, and whether the data was tampered with or edited. All FTC staff and all contractors with network access receive privacy training on an annual basis. Relevant staff and contractors in RIM 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.
Information in the E-Filing system, including nonpublic filings, will be viewed or altered by unauthorized parties.	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

Risk	*Mitigation Strategy*
	documents. Access to documents in the system is granted only to authorized RIM staff and contractors for processing, review and administration, on a read-only basis to authorized OS and OALJ staff. As noted earlier, Attorneys of Record (i.e., complaint counsel and counsel for respondents) have only limited, read-only access to system docket sheets showing the history and status of their filings. Because authorized RIM staff and contractors (including ICF 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, Attorneys of Record (i.e., complaint counsel and counsel for respondent) and/or third-party participants cannot access any filings (including their own) maintained in the system once such documents are submitted to the system, which only RIM staff and contractors, OS staff and OALJ staff can view. Further, as noted earlier, third-party participants may not receive service through the E-Filing 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.

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

Yes, after three unsuccessful attempts, the system automatically locks the user out of their account. Access will be restored after the user contacts the E-Filing help desk and verify that they are the user. Additionally, the system automatically logs the individual's username and activity when information is moved, modified, or deleted.

Further, because authorized RIM 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, Attorneys of Record (i.e., complaint counsel and counsel for respondent) and/or third-party participants cannot 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 RIM staff and contractors, OS staff and OALJ staff can view the documents.

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, copies of public filings posted on the FTC Web site are covered by FTC I-6 (public records). All filings received through the E-Filing system are maintained in that system (separately from any public copies that may be posted on the FTC Web site) and covered by FTC I-1 (investigational and other nonpublic FTC program records). System user data are covered by FTC VII-3. All FTC SORNs are available online.

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 collection, use, and disclosure of information in the system have been reviewed to ensure consistency with the FTC's privacy policy. Periodic reviews are conducted to ensure that use of the system is consistent with FTC's privacy policy.

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Jack Gabriel
Customer and Project Management Office

Reviewed By:

_____ **Date: _____**
John Krebs
Acting Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____**
Jaime Vargas
Chief Information Security Officer (CISO)

_____ **Date: _____**
Yvonne K. Wilson
Records and Information Management Office (RIM)

Approved By:

_____ **Date: _____**
Raghav Vajjhala
Chief Information Officer (CIO)