Table of Contents

1 SystemOverview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) has updated its system for receiving and managing electronic filings in FTC administrative proceedings under Part 3 of its Rules of Practice, by incorporating a web-based application developed on the ServiceNow platform.[1] Part 3 sets forth the procedures for competition and consumer protection cases tried before an Administrative Law Judge (ALJ) of the FTC, and appeals of the ALJ's initial decision to the full Commission. During Part 3 proceedings, electronic filings and public documents are received and served electronically.

Administrative E-Filing, or Admin E-Filing, allows users to submit public and nonpublic pleadings and motions in Part 3 administrative litigations before the ALJ and the Commission. Submitting these documents electronically speeds up the process for circulating these filings to the relevant offices within the Commission and reduces costs incurred for scanning and courier use.

In order to use the Administrative E-Filing application, a user (i.e., lawyers representing respondents or third parties in the Part 3 matter) must register with a unique user ID and password. The user's name, company name, work address, work telephone number, work email address, and bar admission number (if applicable) are required to register. The user is then required to enter a Notice of Appearance in a specific administrative litigation.[2] Once

0 6.48.75.77.76 2

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII) [3] 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
- ☐ Date of Birth
- ☐ Home Address
- ☒ Phone Number(s)
- ☐ Place of Birth
- ☐ Age
- ☐ Race/ethnicity
- ☐ Alias
- ☐ Sex
- ☒ Email Address
- ☒ Work Address
- ☐ Taxpayer ID
- ☐

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

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-

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.

Yes, FTC contractors will have access to data in the system. Contractors must use FTC issued laptops to access the system, using their PIV cards. All FTC contractors are required to sign non-disclosure agreements (NDA), complete security and privacy training prior to obtaining access to any FTC systems, and complete annual security and privacy training to maintain network access and access to those systems.

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.

FTC contractors with access rights to the ServiceNow E-Filing application are subject to the same rules and policies as FTC staff, including adherence to the FTC Breach Notification Response Plan.

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.

☐

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

Yes. Individuals can log into their account and access limited personal information about themselves, such as their password and security questions. They do not have the ability to change their profile information or access log details about their activity. An individual may make a Privacy Act request to the FTC for access to additional information maintained about them in the ServiceNow Admin E-Filing application. See Commission Rule 4.13 (Privacy Act request procedures). Access to the information under the Privacy Act may be subject to certain exemptions. See Commission Rule 4.13(m). Individuals may also file Freedom of Information Act (FOIA) requests for agency records about them (if they are not exempt from disclosure to them under those laws). 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.

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. The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC, including any information that may be stored in the ServiceNow Admin E-Filing application. As stated above in 4.3, individuals can file requests with the FTC under the FOIA and the Privacy Act for access to any agency records that may be about them and are not exempt from disclosure to them under those laws. 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.

The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

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?

It is incumbent upon the person submitting the filing to ensure that the information contained therein is accurate and up to date. Additionally, all Notices of Appeal submitted

filings that are not in compliance are returned/rejected

6 Data Retention and Disposal

6

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
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users r agree to the FTC Rules of Behavior, which includes consenting to monitoring and restrictions on data usage.
Unauthorized system access	All FTC users must have an FTC account and governmentissued personal identity verification (PIV) card to access ServiceNow. FTC's user identity management processes include authentication with enterprise directory to control and manage access restrictions to authorized personnel on an
	official needto-know basis. The FTC utilizes a combinatio of technical and operational controls to reduce risk in the ServiceNow environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, ServiceNow undergoes regular reviews of its security controls. External users will be required to authenticate using twofactor authentication: username/password and OTP passcode delivered to user (voice or token authenticator app on their smartphone).
Data leakage	Non-FTC ServiceNow system administrators are not allow to review, audit, transmit, or store FTC data, which minimizes privacy risks from the vendor source.
Eavesdropping	The users interact with the Admin-Filing application over the TLS protocol (https), an authenticated protected chan

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

The Admin E-Filing application inherits all privacy controls from the parent ServiceNow application. This includes an automatic logoff after 15 minutes of inactivity, deactivating users after 35 days of account inactivity, and locking user accounts after 3 incorrect password attempts. External users can only view and access information and data that they have

submitted into the application. External users can only file attachments after their Notice of Appearance (NOA) has been approved by an OS administrator.

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).

Information collected about users from their Notices of Appearances is considered part of FTC VII-3 -- Computer Systems User Identification and Access Records – FTC. Pleadings or other filings and documents submitted by users through the system are part of FTC I-1 - Nonpublic Investigational and Other Nonpublic Legal Program Records – FTC. To the extent such pleadings or other documents are placed on the public record of the Part 3 administrative proceeding (i.e., posted on the FTC's public web site), such materials are part of FTC I-6 -- Public Records -- FTC. These SORNs may be read and downloaded at https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems.

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 administrative and technical controls described in section 5.2 of this document provi1-2 ()-1 (o)