



Federal Trade Commission
Privacy Impact Assessment

FOIAXpress

Updated February 2018

Table of Contents

1 System Overview 3

2 Data Type, Sources, and Use 4

3 Data Access and Sharing..... 7

4 Notice and Consent 9

5 Data Accuracy and Security..... 11

6 Data Retention and Disposal..... 13

7 Website Privacy Evaluation 13

8 Privacy Risks and Evaluation 14

9 Approval and Signature Page..... 16

1 System Overview

1.1 Describe the project/system and its purpose.

This Privacy Impact Assessment (PIA) describes and assesses privacy risks related to the Federal Trade Commission's (FTC) FOIAXpress system. The FTC's Office of General Counsel (OGC) uses this electronic system to track and fulfill requests filed by members of the public seeking access to nonpublic FTC records under the Freedom of Information Act (FOIA), and requests from individuals seeking access under the Privacy Act of 1974 (PA) to nonpublic FTC records, if any, about themselves. This PIA explains what information about individuals is maintained in the FOIAXpress system, how we collect that information, who is allowed to use it and for what purposes, and what steps the FTC has taken to identify, secure, and reduce any privacy risks to that information.

The FOIAXpress system is a commercial off-the-shelf web-based application owned and operated by AINS Inc.; AINS administers and maintains the software application and all physical systems and securely hosts FTC data. FTC staff access FOIAXpress through a secure website available only on the FTC network. The system allows the FTC to log and track the processing of each FOIA or PA request, using data entered by FTC staff or automatically generated by the system about the request, the requester, or the FTC staff assigned to process the request. The system records the status of the request, relevant deadlines, and other key events or data, such as the dates that actions occurred. The system also stores internal and external correspondence, such as memoranda to supervisors, requests for records sent to staff, and communications with the requester. The FTC also uses FOIAXpress to store and manage copies of the nonpublic agency records that have been gathered in response to each access request. In some cases, these copies contain personally identifiable information (PII) about the requester or about other individuals mentioned or discussed in the records. Authorized system users can use optical character recognition (OCR) to search within records saved in FOIAXpress to locate information from multiple requests that may also be responsive to new requests.

The FOIAXpress system includes the Public Access Link (PAL), a web portal that allows members of the public to electronically submit and track the status of their FOIA or PA requests. PAL has a payment connector, Pay.gov¹, which enables the FTC to accept online payments for FOIA processing. Individuals can create a PAL account with a unique login ID and password and submit requests for information electronically through a link on www.ftc.gov. Requesters may also attach supporting documentation to their request and directly download the documents through PAL if/when the documents are released by the FTC. The PAL portion of FOIAXpress is publicly accessible through the Internet; however, requesters do not have the ability to directly access the FOIAXpress system or other data stored in the system. Only authorized FTC FOIA/PA personnel have access to the data supplied by requesters via FOIAXpress.

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

The FTC's collection and maintenance of information in FOIAXpress relating to FOIA and PA access requests is authorized by the FOIA, 5 U.S.C. § 552, as amended, and the Privacy Act of 1974, 5 U.S.C. § 552a, both of which require the FTC to respond to requests and appeals filed under those

¹ Pay.gov is an U.S. Department of Treasury service that provides connectivity with third-party payment providers. This payment connectors provides requesters with an easy way to submit payment, ensures government recovery of process expenses, and speeds up responsive document delivery. See [Treasury PIA for Pay.gov](#) for more information.

statutes. See also 16 C.F.R. §§ 4.11 and 4.13 (FTC rules implementing the FOIA and PA, respectively). The FOIA, the PA, and the Federal Records Act, 44 U.S.C. § 3301 et seq., require that responsive records be temporarily or permanently maintained. Certain information is also needed to generate annual reports to the Department of Justice as required by FOIA. Information, including PII, in responsive documents saved in the system is collected under, and its handling governed by, other laws and regulations (e.g., FTC Act), as discussed in Section 2 below.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)² may be collected or maintained in the system/project. Check all that apply.

<i>PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.</i>		
<input checked="" type="checkbox"/> Full Name	<input type="checkbox"/> Biometric Identifiers (e.g., fingerprint, voiceprint)	<input checked="" type="checkbox"/> User ID
<input checked="" type="checkbox"/> Date of Birth	<input type="checkbox"/> Audio Recordings	<input type="checkbox"/> Internet Cookie Containing PII
<input checked="" type="checkbox"/> Home Address	<input type="checkbox"/> Photographic Identifiers (e.g., image, x-ray, video)	<input checked="" type="checkbox"/> Employment Status, History, or Information
<input checked="" type="checkbox"/> Phone Number(s)	<input type="checkbox"/> Certificates (e.g., birth, death, marriage, etc.)	<input type="checkbox"/> Employee Identification Number (EIN)
<input type="checkbox"/> Place of Birth	<input type="checkbox"/> Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	<input type="checkbox"/> Salary
<input type="checkbox"/> Age	<input type="checkbox"/> Vehicle Identifiers (e.g., license plates)	<input type="checkbox"/> Military Status/Records/ ID Number
<input type="checkbox"/> Race/ethnicity	<input checked="" type="checkbox"/> Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	<input type="checkbox"/> IP/MAC Address
<input type="checkbox"/> Alias	<input type="checkbox"/> Geolocation Information	<input type="checkbox"/> Investigation Report or Database
<input type="checkbox"/> Sex	<input type="checkbox"/> Passport Number	<input checked="" type="checkbox"/> Driver's License/State ID Number (or foreign country equivalent)
<input checked="" type="checkbox"/> Email Address		<input checked="" type="checkbox"/> Other (<i>Please Specify</i>): Passwords
<input checked="" type="checkbox"/> Work Address		
<input checked="" type="checkbox"/> Taxpayer ID		
<input checked="" type="checkbox"/> Credit Card Number		
<input checked="" type="checkbox"/> Facsimile Number		
<input type="checkbox"/> Medical Information		
<input type="checkbox"/> Education Records		
<input type="checkbox"/> Social Security Number		
<input type="checkbox"/> Mother's Maiden Name		

Requester Profile. Individual requesters can set up their own accounts and electronically submit FOIA/PA requests via the PAL web portal. In order to set up a PAL user account, an individual may provide his/her full name, telephone and/or fax number, home address, email address, job title, and organization name. The PAL portal logs requesters' user names and passwords. For individuals that submit FOIA/PA requests via hardcopy mail, email, or telephone, OGC staff create profiles in FOIAXpress on behalf of the requester and enter the individual's contact information. Individuals can also submit FOIA requests using the FTC's online [FOIA request form](#), which OGC staff can use to create a requester profile in the system. This information can include the requester's name, address, telephone and fax numbers, email address, job title, and organization name, as well as a requester's FOIA fee category, which is selected by staff. System users can search and retrieve Requester Profiles using any of the PII entered in the profile fields.

² 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.

Request Profile. Each request logged in FOIAXpress has a Request Profile containing information about the request. The Request Profile imports PII from the relevant Requester Profile, including the requester's name and contact information. The Request Profile also maintains relevant dates, fee information, and a description of the request. If a request involves documents pertaining to a specific individual, that individual's name (which may be different than the requester's) may appear in the request description; however FOIA/PA staff generally avoid this scenario. The request description may provide contextual information about the requester. For instance, if the request description reads "Requester's own complaint", the fact that the requester submitted a consumer complaint (and therefore likely considered him- or herself a victim of a scam), will be suggested.

Correspondence Log. Communications (e.g., letters, e-mails, and facsimiles) to and from the requesting party are saved as electronic files in the correspondence log portion of the system. PII captured in correspondence can include, but is not limited to, names, addresses, telephone numbers, e-mail addresses, fax numbers, and other contact information of the requester or the person filing on behalf of the requester. It is OGC policy to redact Social Security numbers, dates and places of birth, photographic identifiers, and/or driver's license/State ID numbers from documents before they are saved in the correspondence log section of the system, as described further in Section 8.1.

File Cabinet/Document Management. As noted above, the system also maintains copies of materials responsive to the access request that have been gathered from FTC offices and saved in the system. These documents consist of legal, investigatory, administrative, or similar nonpublic agency records, some of which may contain PII about investigatory targets or other individuals (e.g., witnesses, complainants, FTC staff, other consumers, or the requester) depending on the type and nature of the record. For example, such PII can include names, addresses, telephone numbers, or other information about an individual (e.g., a complaint by a consumer or description of an alleged violation by the subject of the investigation). System users can use an Optical Character Search ("OCR") feature to locate responsive PII within Document Management (this full-text search feature cannot be used to search any other portion of the system.).

Review Log and Request Folder. Once responsive records within Document Management are redacted by a FOIA Professional they are sent to the Review Log section for supervisory review and approval. After redacted records are approved for an outgoing response to the requester, the records are sent to the Request Folder before delivery to the requester. The documents found within the Review Log and the Case Folder are copies of documents in Document Management, with redactions applied.

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.

The FOIAXpress system maintains copies of materials responsive to the access request that have been gathered from FTC offices and saved in the system. The system thus contains the various types of records that are generated, received, or maintained by agency staff. These documents consist of legal, investigatory, administrative, or similar nonpublic agency records, which may contain law enforcement-related or confidential commercial information, or other types of sensitive non-PII obtained from outside parties, investigatory targets, or other individuals (e.g., witnesses, complainants, FTC and staff from other government entities or Congress, other consumers, or the requester), depending on the type and nature of the record.

FTC OGC Staff – FOIAXpress also stores information on the identity of system users. For example, FOIAXpress maintains information about FTC staff with password-protected access as explained in

Section 3, including their name and official contact information, and the specific access requests they worked on. FOIAXpress maintains records showing who has access, who the active users are, and what access requests the users have been assigned to process.

Other FTC Staff – FOIAXpress stores information about other FTC staff who serve as FOIA/PA liaisons for their respective offices. This information includes the employee’s name and official contact information, such as their FTC address, phone number, and email address.

FOIA Requesters (via PAL) – FOIAXpress maintains information pertaining to the requester to include the subject matter of the request, the requester’s organization (if applicable), the FOIA number associated with the request, as well as the OGC staff member assigned to the request. The PAL portal also maintains additional log data relating to the requester, such as IP address, time, date, and browser type.

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

The information collected in the system is used to respond to access requests under the FOIA or the PA, to track these requests in order to maintain compliance with statutory response times, and to maintain documents responsive to these requests in compliance with legal retention and disposition schedules, including any records that are exempt from disclosure to the requester under the FOIA or the PA. The information is also used to generate annual reports to the Department of Justice (DOJ) as required by FOIA.

2.4 What are the sources of the information in the system/project? How is the information collected?

<i>Source of Data</i>	<i>Type of Data Provided & How It Is Collected</i>
Individual requesters	Requesters must provide enough information to reasonably describe their request, verify their identity and contact information, and agree to pay the appropriate processing fees. The information provided can include name, address, telephone and fax numbers, email address, job title, and organization name. A request is not properly filed unless these criteria are met. Individuals may submit FOIA requests through the PAL web portal by creating a user profile and setting an account password. Requesters may also directly contact the FTC via mail, email, or telephone and provide the information necessary to create a requester profile in FOIAXpress.
FTC FOIA/PA staff	FTC officials may enter additional information when appropriate or necessary to ensure that a FOIA request is properly filed or amended in the course of processing, considering, and responding to these access requests (e.g., notes about when staff discussed the request with the requester). FTC staff may also enter information related to system users and FOIA/PA liaisons, such as names, official contact information, and user ID and password. The names and contact information of FTC users and FOIA/PA liaisons are provided by the users or liaisons themselves, or by other staff in their organization.

<i>Source of Data</i>	<i>Type of Data Provided & How It Is Collected</i>
FOIAXpress	<p>Some information in the system is generated or compiled by the system itself (e.g., deadlines for responding to an individual's FOIA request; date, time and other information about actions taken within the system).</p> <p>Additionally, the PAL portal collects the requester's user ID and password and logs the user's IP address, time, date, and browser type.</p>
Responsive Records	<p>Certain records in the system consist of documents that have been identified as responsive to access requests. Such records (e.g., affidavit, court filing, investigatory record, personnel file), which may include PII or confidential commercial information, will have come from the individual requester, from some other individual (e.g., investigatory targets, witnesses, consumer complainants, employees), or from other sources (e.g., other government entities, news media, commercial databases, companies, or non-individual entities).</p>

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.

<i>Data Will Be Accessed By and/or Provided To:</i>	<i>How and Why the Data Will Be Accessed/Shared</i>
FTC OGC Staff	<p>Professionals within the FTC's OGC have User ID and password-protected access to the records as necessary to perform administrative functions (e.g. create Requester Profiles, log incoming FOIA/PA requests), prepare responses to FOIA/PA requests and appeals, and to prepare periodic reports as required by law, executive order, or agency directive.</p>
Other FTC Staff	<p>Intermittently, staff in other FTC Divisions and Offices (e.g., Office of the Inspector General or OIG) may be granted access rights to the FOIAXpress system. This occurs in limited situations and for a specified reason, and they must receive a User ID and password before access is granted. System users may share information maintained within the system (e.g., requester contact information, PII existing within responsive records) with other FTC staff, including FOIA/PA liaisons and record custodians, as necessary to search for and to appropriately review and redact responsive records prior to release.</p> <p>OGC Information Technology (IT) and administrative staff and staff and contractors in the FTC OCIO have access as necessary to administer and support FOIAXpress operations.</p>
AINS Staff	<p>Authorized AINS staff have access to FOIAXpress for general system maintenance purposes, such as implementation, upgrades, and troubleshooting, as required.</p>

Note: Members of the public do not have access to the FOIAXpress system, other than access to

the PAL web portal, which allows them to create a user profile, submit, and track the status of their FOIA/PA requests. They do not have access to request records in FOIAXpress or other data stored in the FOIAXpress 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.

FTC IT contractors will not have access to the system unless it is necessary for the administration and processing of access requests, or to ensure the proper functioning of the system. In that case, specific access will be granted and removed when the necessary work has been completed. FOIA/PA requesters have access to responsive records in the system only when OGC staff retrieve them from the system and disclose them in electronic or paper format to such requesters. Before such disclosure, staff may share such documents with other government agencies, Congress, or the records' original submitters in order to determine whether the materials are confidential or otherwise exempt from mandatory FOIA or PA disclosure. In addition, as noted earlier, the PA also allows the FTC to disclose records that have been saved in the system for other "routine uses" compatible with the purpose for which the records were collected, as set forth in the applicable Privacy Act SORNs. See Section 8 below.

Authorized AINS staff have access to servers containing FTC data to perform maintenance and troubleshooting activities; these staff have signed the appropriate non-disclosure agreements with the FTC. They are also required to take the company's annual security training as a condition of employment. FTC data within the FOIAXpress system is encrypted and not generally accessible to AINS staff.

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 that have access to the FOIAXpress system are subject to the FTC's policies, procedures and practices as a condition of employment. This includes mandatory Information Security and Privacy Training that must be completed on an annual basis and a requirement to abide by and follow procedures outlined in the FTC's Data Breach Response Plan.

AINS maintains its own incident response plan, which outlines procedures for reporting information security incidents, including communications, restoring services, and providing breach notifications. The FTC's contract with AINS requires the company to immediately notify the agency of any breaches that may affect FTC data.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

- Notice is provided via (*check all that apply*):
- Privacy Act Statement (Written Oral)
 - FTC Website Privacy Policy
 - Privacy Notice (e.g., on Social Media platforms)
 - Login banner
 - Other (*explain*): _____

Notice is not provided (explain): _____

The FTC notifies the public, including FOIA/PA requesters, and FOIAXpress system users, administrators, and other FTC staff about what information is collected in the system, and how it is used and disclosed, through applicable system of records notices that the FTC has published in the *Federal Register* and posted [online](#). As required by the FOIA, the Commission also sets out in its regulations at 16 C.F.R. § 4.11 and in the agency's [FOIA Handbook](#) what information the FTC needs from a requester to process an access request. The FTC also provides a Privacy Act Statement on the online [FOIA request form](#) as well as on the PAL portal to notify users of the collection of personally identifiable information.

In contrast, notice to individuals whose information may be contained in responsive documents saved in the FOIAXpress system is provided to such individuals, where appropriate or legally required, at the time that information is collected from him or her (e.g., by subpoena, civil investigatory demand, or other compulsory process, by voluntary access request in an investigation). In some cases (e.g., court cases), an individual may also receive notice when the FTC collects his or her information from other sources (e.g., when the FTC serves a subpoena on another person or entity for information about the individual and the court rules require the FTC to notify that individual as well).

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)?

FOIA/PA requesters: All information provided by FOIA/PA requesters to the FTC is voluntary. Requesters may freely decline to provide any information they do not wish to provide; however, such a refusal may adversely affect the FTC's ability to process a FOIA or PA response if the contact information is inadequate or the individual's identity cannot be authenticated.

Requesters do not have a right to consent to the particular use of information provided in a FOIA request. Under the Commission's Rules of Practice, 16 C.F.R. § 4.9, FOIA requests and response letters denying or granting access are a part of the FTC's public record. The FTC may redact certain PII from a FOIA request, such as the requester's address or telephone number, before making it publicly available, in order to protect elements of the requester's privacy. In addition, requesters can complete and submit a certification of identity to OGC staff authorizing other individuals (e.g., personal attorney) to file FOIA/PA requests on their behalf and to obtain copies of the agency records that have been requested.

PA requests and response letters are not part of the public record. PA requesters must provide written

consent before their information can be shared, except as authorized by the Privacy Act (i.e., within the agency to officials who require access for performance of duties, as required by FOIA or as authorized by routine uses).

FOIAXpress system users and administrators: System users must enter their user ID and passwords (in the login screen) in order to access the FOIAXpress system. If the user declines to provide this information, the system does not grant access. The user has no right or opportunity to decline to provide other information, such as their name and contact information or usage data in the system (e.g., date, time of user session), which is generated and maintained automatically by the system itself.

These individuals do not have a right to consent to or otherwise determine how the agency uses their name or contact information, or the information collected by the system regarding their login, access, or use of the system.

Other individuals: The right or opportunity of individuals to provide information that is contained in responsive documents saved in the FOIAXpress system depends on how the information was collected and whether applicable laws or other legal authorities give the individual a right or opportunity to decline to provide the information. In some cases, individuals will have the right to decline to provide information (e.g., voluntary requests), while in other cases, individuals have no such right (e.g., subpoenas), although they may have the legal right in those cases to challenge the request (e.g., by filing a motion to quash the subpoena).

Individuals who have provided information in agency records that have been saved in the FOIAXpress system for disclosure to a FOIA/PA requester do not have rights to consent to such use. The FOIA and PA legally determine whether the FTC is required to disclose, or whether it may withhold, such records from a requester seeking access under those laws.

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

Individuals may file an access request under the PA or the FOIA, depending on how the information is maintained and retrieved. The PA provides a procedure for individuals to request their own information, if the agency maintains and retrieves that information by the individual's name or other personal identifier (e.g., Social Security number). The FTC's Privacy Act procedures are published at 16 C.F.R. § 4.13.

The request must be made in writing and, if mailed, it must be addressed as follows:

Privacy Act Request
Office of the General Counsel
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

PA Requests may also be made electronically using the FTC's online [FOIA request form](#).

If information about an individual is not maintained and retrieved by his or her name, Social Security number, or other personal identifier, the individual's request must be made under the FOIA, rather than the Privacy Act. The procedures for making a FOIA request are similar to making a Privacy Act request, and are published at 16 C.F.R. § 4.11. Individuals who use the FTC's online FOIA request

form to file a PA or FOIA request will also have their request treated as a FOIA request for any records that fall outside the PA.

Requesters should note that some records may be legally withheld from individuals for investigatory or other reasons under the FOIA and/or the PA. *See* Section 8 of this PIA for additional details.

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.

See Section 4.3. Rule 4.13(g)-(h), 16 C.F.R. 4.13(g)-(h), provides procedures for individuals to request a correction or amendment of records about themselves and for the agency to review such records. After the agency makes the initial determination pursuant to Rule 4.13(h), there are appeal procedures in Rule 4.13(i) allowing for the appeal of an initial adverse agency determination. As noted below, see section 5.1, FOIA staff may consult directly with the FOIA requester to clarify, correct or otherwise amend the FOIA request to ensure that it accurately reflects the intended scope of the request and to help ensure that the request is processed in a proper and timely fashion.

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?

Information stored in the system about requesters has been collected from the requesters themselves (i.e., through their access requests and related communications) or is generated and entered by staff. OGC staff check the accuracy and timeliness of this information (e.g., contact information, precise scope of the request) as necessary to allow FTC staff to respond to or contact a requester and to ensure that FTC staff accurately interpret and respond to the request. Furthermore, as set out by 16 C.F.R. § 4.13, when the request is from an individual seeking access to his or her own records under the Privacy Act (e.g., a consumer seeks a copy of a complaint he or she previously submitted, or an FTC employee seeks access to or a copy of his or her own personnel records), OGC staff may require additional verification of that requester's identity when reasonably necessary to assure that records are not disclosed to someone other than the submitter or the submitter's representative.

OGC staff does not check the accuracy or timeliness of information, including PII, contained in responsive documents that are saved in the system. The FTC is required under the FOIA to grant or deny access to responsive records "as is," without alteration. The accuracy and timeliness of the information (including any PII) contained in such records, would be governed by other laws and authorities, if any, applicable at the time the agency compiles those records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures), or by the Agency's Privacy Act procedure for correcting or amending records, discussed above.

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.

Access Restrictions: Access to nonpublic records saved in the system is restricted to FTC personnel or contractors whose responsibilities require access, i.e., OGC's FOIA/PA staff. The FOIA/PA Program Director (the Assistant General Counsel for Information and Litigation Support) must authorize access to any new user. New requests for access are then submitted to the Enterprise Service Desk (Help Desk) within the FTC's Office of the Chief Information Officer, which loads the software onto the new user's machine.

Currently, the Program Director, senior attorneys, and an information technology specialist are the only users with administrative privileges. A user with administrative privileges creates an account for new users and assigns them to a group. Each user group has different privileges, and the FOIAXpress system has the capability to grant privileges on a user level. The FOIA user group, which contains all FOIA specialists, does not have administrative rights. Therefore, they cannot engage in administrative processes such as creating user names, changing passwords, or changing the fee structure. FOIAXpress also maintains information on the identity of system users (those with password protected access), including the specific access requests they worked on. The system also has the capacity to employ additional audit trail procedures about system users and to track activity on specific FOIA requests as necessary.

FTC data in FOIAXpress is encrypted at the database level; AINS staff do not have direct access to FTC data in the system.

Training: All FTC personnel, including those FOIA/PA Professionals who use FOIAXpress, are subject to FTC procedures for safeguarding PII. All FTC personnel receive annual computer-based privacy and security training, as well as other guidance explaining how to safeguard information. The interactive online training covers topics such as how to properly handle sensitive PII and other data, online threats, social engineering, and the physical security of documents. In addition, all FOIA/PA professionals comply with the Agency's internal procedures for safeguarding sensitive PII, which ensures such information is handled appropriately. Furthermore, persons at the FTC with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

In addition, each FOIA/PA professional also takes periodic training on FOIA and Privacy Act issues provided by approved outside sources (e.g., Department of Justice, Department of Agriculture Graduate School, American Society of Access Professionals).

Other Physical and Security Controls: Additionally, nonpublic paper records are retained temporarily, maintained in lockable file cabinets or offices, and returned to the submitter or destroyed once the request is complete. Access to all electronic records within the Agency is controlled by "user ID" and password combination and other electronic access or network controls (e.g., firewalls). As noted above, FOIAXpress users have an additional "user ID" and password protected entry point into the system. FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. These and other information and physical security measures currently in place are subject to periodic reviews and audits by the Commission's Inspector General.

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

FOIAXpress is a subsystem within the eCase suite of applications. A risk assessment for eCase was completed and an Authorization to Operate is scheduled to be granted in March 2018. FOIAXpress is a subsystem of eCase.

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?

Records are retained and disposed of in accordance with General Records Schedule 4.2, issued by the National Archives and Records Administration (NARA).

The Retention Policy Management module in FOIAXpress will allow the FOIA team to create, safeguard, access records and archive or dispose them according to the General Records Schedule 4.2: Information Access and Protection Records, issued by NARA. The retention policy is created at the Administrative Retention Miscellaneous Fields and will be applied only to closed request folders. When closing a request folder, the system will set the retention expiration date based on the retention policy configuration (6 years after final agency action or 3 years after final adjudication by the courts, whichever is later).

Additionally, the system will verify whether any open appeal or litigation matters exist for the closed request. In such instances, the system will not allow users to mark the request for deletion.

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.

Authorized FTC staff and contractors access FOIAXpress through a secured website that has been set up specifically for the FTC's use. FTC personnel use a specific URL to access FOIAXpress from the FTC or remotely; this URL is not otherwise publicly available on the Internet. FOIAXpress uses temporary session cookies to track user sessions in the web browser. There are no persistent cookies in use.

The PAL web portal is integrated with the FOIAXpress system; it is a secure public-facing website that allows members of the public to electronically submit FOIA/PA requests. PAL uses temporary session cookies to track user sessions; persistent cookies are not used on the PAL portal.

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?

The main privacy risk associated with using FOIAXpress to collect and maintain information related to FOIA and PA requests is that sensitive PII present in the requests themselves or in responsive records saved in the system may become compromised by unauthorized use or disclosure.

To mitigate these risks, the FTC has taken steps to minimize the amount of information that the agency collects and maintains about such individuals. For example, the FOIA Office only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests; the FOIA Office does not ask requesters to provide sensitive information (like Social Security Numbers) from requesters. If a requester includes SSNs or birth dates in his/her access request, FOIA professionals redact the unnecessary sensitive information before uploading to FOIAXpress. In limited circumstances, if a document that is responsive to a FOIA request is determined by OGC to be especially sensitive (e.g. containing OIG, personnel, or investigative records), it may not be saved in the system, but rather stored in hard copy under lock and key or in a network storage location with limited access permissions.

To avoid unauthorized access or disclosure, FOIA/PA staff follows agency procedures for storing, sharing, sending, transporting, logging, and destroying sensitive personal information. Access to FOIAXpress is limited (by software licenses) to a small number of specified FTC professionals who need system access to do their jobs. Users may access FOIAXpress only after entering a unique user ID and password, which they must change every 60 days. Only the user and FOIA professionals with Administrator rights can change these passwords.

Furthermore, when the FTC provides documents in response to an access request, the FTC redacts personal information from the documents where the information, if publicly disclosed, would cause a “clearly unwarranted invasion of personal privacy.” *See* 5 U.S.C. § 552(b)(6). When a requester is seeking his or her own information under the Privacy Act, the FTC verifies the individual’s identity as required in 16 C.F.R. § 4.13 before disclosing the Privacy Act records to him or her. Also see Section 5.1.

An additional potential privacy risk could arise when certain information is extracted from the system for placement on the public record (*See* Commission Rule 4.9(b), 16 C.F.R. § 4.9(b), for a list of all FTC public records, which includes copies of FOIA requests). Personal addresses and telephone numbers are redacted prior to placing the information on the public record, as is more sensitive PII that may be included in the request. FOIA/PA staff also redact a requester’s name when the record requested (e.g., a consumer complaint the requester submitted) would tend to reveal personal information that could cause embarrassment or other harm (e.g., that the requester was the victim of a scam).

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

System users only have limited access privileges to review FOIA requests within FOIAXpress. System users also are locked out after a pre-set number of failed attempts or after a pre-set period of inactivity.

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).

Records pertaining to FOIA/PA requesters are covered by:

V-1 – Freedom of Information Act Requests and Appeals – FTC, and V-2 – Privacy Act Requests and Appeals – FTC.

Records pertaining to FOIAXpress system users are covered by:

VII-3 – Computer Systems User Identification and Access Records – FTC.

Records pertaining to individuals whose information may be retrieved from some documents that have been saved in the system for release to requesters would be covered by:

I-1 – Nonpublic Investigational and Other Nonpublic Legal Program Records– FTC, I-6 – Public Records–FTC, or other applicable FTC SORNs.

All FTC SORNs can be viewed and downloaded [on the FTC website](#).

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 the information in this system has been reviewed to ensure consistency with the FTC’s privacy policy. Additionally, the online FOIA request form links to the FTC [Privacy Policy](#), explaining what the FTC does with personal information that it may collect and maintain on individuals.

9 Approval and Signature Page

Prepared By:

_____ Date: _____
Darrick Latimer
FOIA Technology and Information Specialist
Office of General Counsel (OGC)

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 Filing Office (RFO)

Approved By:

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