Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1505784
PIA Name:	OS - FOIAXpress - QTR4 - 2022 - OS1252401	**Title:**	FOIAXpress
OpDiv:	OS		

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	None.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The Freedom of Information Act Xpress System (FOIA Xpress) is a FOIA request tracking and management system owned by the Assistant Secretary for Public Affairs (ASPA). The purpose of the system is to enable ASPA's FOIA Division to efficiently receive, track, and respond to records requests and appeals made under the Freedom of Information Act (FOIA) and Privacy Act (PA). FOIA Xpress is a Software-as-a-Service (SaaS) cloud application maintained by AINS. FOIA Xpress is part of the AINS eCase suite which functions as the baseline for the application. The eCase platform is a FedRAMP certified platform and provides an automated information management, tracking, and reporting solution. The solution components include the FOIAXpress application and the Public Access Link (PAL) application and the HHS Database Sever. The FOIAXpress database server stores the metadata of the cases. Database server is in FedRAMP boundary and managed by AINS. The PAL application is a public-facing web portal that integrates with FOIAXpress and allows the public to submit and track the status of FOIA requests.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is	The system collects the following information below, which is entered by users or results from system processing of information entered: -

stored.

FOIA/PA requests and appeals received in the

OS FOIA Office by mail, phone, or fax, or online through the system's Public Access Link (PAL), from individual and entity requesters or by referral from another FOIA office (containing requester/appellant name, contact information, and description of records requested and issues raised on appeal); - Responses to requests and appeals (containing requester/appellant name, mailing or email address, summary of request history, number of pages of responsive records located, released, and pages or portions withheld, explanation of exemptions applied, the agency's decision on any appeal issues, and notice of appeal rights); - Intra- and inter-agency communications about requests (containing contact information for agency personnel and the requester/appellant and any information conveyed, pertaining to issues such as which offices could have responsive records, search or processing status, types and quantities of records located, reasons for delays, and estimated time-frames); - Clean, marked, and redacted copies of responsive records processed for release (which could be any agency record on any topic, containing any type of Personally Identifiable Information (PII), depending on the request); - Case tracking information (containing requester/appellant name, case tracking number, and processing stages such as date request received, date response due, number of days overdue, whether response deadline is tolled (stopped), date records received, date response letter submitted for signature, date response provided, FOIA Analyst assigned to request); - Form letters and report templates (these do not contain PII); - Fee-related records (containing fee estimates and discussions or decisions about fees and fee waiver/reduction requests); - Statistical and narrative reports (these do not contain PII); - Internal productivity reports (some include requester/appellant names, descriptions of records requested, and status information that indicates something about a requester); and - user access records (containing personal identity verification (PIV) PIN and FOIAXpress user ID and password for HHS users, which include employees and direct contractors (all direct contractors have HHS-issued PIV cards); and user name and password for members of the public using the Public Access Link (PAL) portion of the system to log into their PAL account). Information from the system is shared as follows:

1) To process requests and appeals, relevant information is shared with: - Agency personnel who route requests, communicate with requesters, locate, review and process responsive records, and prepare, approve, and sign response letters; - Other federal agencies and business submitters that may have an interest in responsive records; - Direct contractors assisting in processing requests/appeals; - Requesters/appellants; and - The Department of Justice to resolve FOIA policy or legal issues.

2) In the event of litigation, information is shared with: - The Department of Justice, courts, and opposing parties.

3) In the event of a mediation or review of HHS' FOIA Program, information is shared with the Office of Government Information Services (OGIS) within the National Archives and Records Administration (NARA).

4) To collect any fees charged to requesters, fee-related information is shared with HHS' financial management system.

5) For FOIA program reporting purposes, statistical (non-PII) information is shared in internal reports and public reports.

6) To trouble-shoot system issues, information may be shared with system contractor (an indirect contractor not issued a PIV card), HHS IT personnel, and direct contractors.

7) To administer user access privileges, user information is shared with the system administrator(s).

8) In the event of a data security incident.

The information is stored in the system for 10 years.

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	FOIAXpress is an all-inclusive system that provides a FOIA Office with all tracking, storage, processing, communication, management, and reporting tools required to administer its FOIA program in accordance with statutory and Department of Justice requirements and best practices. The system includes a Public Access Link (PAL) which is an online portal that allows any member of the public to register to create an account that he/she can use to submit requests online, receive limited status information online, and receive responses and responsive records online. To create a PAL account, the user enters his or her name, an email address, selects a requester category (commercial, educational, public, news media, nonprofit), and enters a username, creates a password, and enters a hint question and a hint answer. PAL notifies a requester via email when information is available within the PAL portion of the system for the requester to access by logging into his or her PAL account with his/her username and password. A registered PAL user has access to only the PAL portion of the system, and only to information he/she submits in PAL or that HHS delivers through the system to his/her PAL account. The information collected in FOIAXpress is received directly from registered PAL users (members of the public) who submit FOIA requests and communications to HHS online; or is received from a requester/appellant, or from an HHS office, or from another agency via mail, email, fax, disk, or from an HHS user's workstation drive and is then uploaded to FOIAXpress by an HHS user; or is created or entered in FOIAXpress by an HHS user. (HHS users include employees and direct contractors.) No information is permanently retained.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	FOIA Xpress is a Software-as-a-Service (SaaS) cloud web application maintained by AINS. The web application enables ASPA's FOIA Division to efficiently receive, track, and respond to records requests and appeals made under the Freedom of Information Act (FOIA) and Privacy Act (PA). The application includes a public-facing web portal that allows the public to submit and track the status of FOIA requests. The application requires public users registration to establish an account before granting access.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 12:	Does the website use web measurement and customization	No

	technology?	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 14:	Does the system have a mobile application?	No
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Email Address Date of Birth Mailing Address Name Phone numbers
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The primary purposes for which PII is used are to document and analyze requests received from individual requesters or that seek records about individuals, locate responsive records about individuals, verify the identity of individual requesters, contact requesters, locate cases in the system (e.g., to manage cases or provide status information to requesters), process responsive records containing PII, maintain clean, marked and redacted versions of the processed records, and document responses to requests, including fee issues.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Secondary uses of the PII are to identify requests from the same requester or that seek records about the same individual(s), to prepare internal productivity and status reports, and to use as examples for training purposes.
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	The Social Security Number (SSN) may be

		contained in some of the pre-existing records processed for release using the system and in some of the requests received in the system. A notice is posted on the public access link (PAL) submission instructions screen to discourage inclusion of SSN in requests; it states "'Do not include your SSN" and explains that, if SSN is needed, HHS will request it later. SSN is very seldom needed because other information almost always exists that can serve the same functions. The functions would be: to verify the requester's identity, locate responsive records, or distinguish between records about individuals with the same name and associate records that are under different names but are about the same individual--but only when no other information will suffice as an alternative to using SSN.
PIA - 6A:	Cite the legal authority to use the SSN.	The Freedom of Information Act (FOIA), as amended (5 U.S.C. 552) and the Privacy Act of 1974, as amended (5 U.S.C 552a) impliedly permit or require use of enumerators or other identifying information when necessary to provide individual requesters with access to their records while avoiding inadvertently releasing records to an individual requester that are about a different individual. Because those program-specific authorities authorize use of an enumerator, Executive Order (E.O.) 9397 as amended by E.O.13478 authorizes SSN to be used as the enumerator.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The Freedom of Information Act (FOIA), as amended (5 U.S.C. 552) and the Privacy Act of 1974, as amended (5 U.S.C 552a) are the correct legal authorities, because all requests for agency records are processed under FOIA, except to the extent they are first-party requests for records from a Privacy Act system of records that are fully granted under the Privacy Act alone. First-party requests for Privacy Act records that are not fully granted under the Privacy Act are processed under both the Privacy Act and FOIA.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Requester/appellant name
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals, 81 FR 17463 (3/29/16), updated at 83 FR 6591 (2/14/18).
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Phone Email

		Online Other Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign Other Federal Entities Other Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet Private Sector Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10C:	Explain why an OMB information collection approval number is not required.	The online request mechanism (PAL) does not constitute an information collection under the Paperwork Reduction Act (PRA) based on PRA definitions of 'collection' and 'information' in 5 CFR 1320.3(c) and (h). The PAL registration screen states that a requester may submit a request using that online method or in any manner that conforms to HHS' FOIA regulations, and enables the requester to provide only limited items (name, contact information, description of records sought, user name/password, hint question/answer).
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Other Federal Agencies & White House - To effect consultations and referrals involving

		individual requesters and/or requested records containing PII. Private Sector - To comply with the submitter notice process with respect to financial or commercial records containing PII – this process shares with the submitter the records that the submitter originally provided to HHS, but may also share the identity of the requester. State or Local Agencies - To ascertain facts (such as the existence of a consultant relationship with a state or local agency) or potential harms (such as to federal deliberative processes) affecting whether a FOIA exemption applies to information involving the state or local agency. Within HHS - To route and process requests, records, and report data containing PII, verify identity of requesters, and locate records pertaining to particular individuals.
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	No agreements authorize information sharing. Department of Justice (DOJ) guidance governs consultations and referrals with other agencies. The White House requires FOIA offices to consult with it on records implicating White House equities. Executive Order 12,600 governs the submitter notice process.
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	Not applicable (N/A). (responses to FOIA and Privacy Act requests are exempt from this requirement per 5 USC 552a(c)(1).)
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	An individual requester can choose which contact information to provide to the FOIA office and which method to use to submit a request (e.g., need not use the online method). A third-party requester can make a request anonymously through a nominee. A first-party requester can limit the type, number, date range, subject matter, etc., of records he/she requests about himself/herself, and need not provide SSN or other identification information if other information is sufficient to locate the requested records and verify the requester's identity. An individual whose PII is in records responsive to a third-party FOIA request has no option to object to the inclusion of the records about him/her in the system.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	Major changes to the FOIAXpress system would be described in a revision to System of Records Notice (SORN) 09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals, which would be published in the Federal Register and posted to the HHS SORN webpage.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process	An individual's concern that his/her PII was inappropriately released to a FOIA requester would be reported within HHS as a privacy

	exists, explain why not.	incident and would be analyzed to determine if an improper disclosure occurred; the concern would be responded to in writing, if appropriate; and remedial measures would be taken if an improper disclosure occurred. Although this system is excepted from the Privacy Act 'accounting of disclosures' requirement, an individual can make a FOIA request for the FOIA request log to identify any individuals and entities requesting records about him/her, a description of the records requested, and the dates of the requests. An individual requester who believes that his/her contact information or other information about his/her request is inaccurate in the system can contact the OS FOIA Office or System Manager identified in SORN 09-90-0058 to request access to the records and contest and seek correction of any inaccurate information. Requesters submitting requests online can update or correct their profile information, including their contact information, at any time.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	HHS system users are instructed to promptly enter or upload into the system any updated profile information, contact information, or other PII that they receive from requesters/appellants.

		The system automatically assigns a unique sequential tracking number to each request and appeal, which includes the fiscal year. The system also sends an immediate, or near-immediate, acknowledgement of receipt to the requester/appellant, documenting the date and time of receipt. Most requesters/appellants know to contact the OS FOIA Office if they fail to receive the acknowledgement; in the absence of a tracking number, receipt/nonreceipt can be confirmed using the requester's/appellant's name, so that any unaccounted for request or appeal can be promptly resubmitted. Staff are reminded regularly (and, in particular, at the end of each Fiscal Year, when statistics are generated for each annual FOIA report) to ensure that concluded cases are closed in the system. The process of closing cases in the system and indicating if a case involves litigation enables the system to calculate disposition eligibility dates so that PII records in the system (and in any associated paper case files maintained for older requests/appeals) can be destroyed when no longer needed. HHS system users are instructed to enter or upload into the system any updated profile information, contact information, or other PII that information they receive from requesters/appellants. The system automatically assigns a unique sequential tracking number to each request and appeal and sends an immediate acknowledgement of receipt to the requester or appellant documenting the date and time of receipt. Requesters/appellants know to contact the OS FOIA Office if they fail to receive the acknowledgement, which alerts staff to any system glitch. Staff are regularly reminded to ensure that concluded cases are closed in the system, and in particular at the end of each Fiscal Year, so that the system will generate accurate statistics for each annual FOIA report. Any paper case files that are maintained (e.g., for older requests/appeals) is periodically compared to printouts of cases in the system to ensure that the tracking numbers match the names, that the requests and paper files are accounted for, and that concluded cases are closed in the system. The process of closing cases in the system and indicating if a case involves litigation (and if so, entering the date litigation was concluded) enables the system to calculate disposition eligibility dates so that PII records (within the system, and in any associated paper case files maintained for older requests/appeals) can be destroyed when no longer needed.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors

PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	No
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	System Users: HHS Users (FOIA Office staff and FOIA Coordinators, including employees and direct contractors) have access to PII pertaining to requests they handle, for purposes of handling the requests. Members of the public who use the Public Access Link (PAL) have access to their own PII in order to update their PAL account information, submit requests and related communications to FOIA staff, and receive responses to same. System Administrators: Administrator-level access is granted only to certain users in the OS FOIA Office and at the system contractor (an indirect contractor not issued a PIV card), and possibly also in the agency's Office of the Chief Information Officer (OCIO). Administrators have access to PII for purposes of maintaining and updating the system, administering user access, and troubleshooting system problems. Contractors: The system contractor (the COTS system owner, AINS, Inc.) has the ability to access, but is not intended to access, PII in the system—other than users' access control records–for purposes of maintaining the cloud storage system and updating the system, administering user access, and troubleshooting system problems. Direct contractors retained to assist the OS FOIA Office in processing requests and appeals have access to PII for purposes of providing that assistance.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All users necessarily must have access to PII, because many of the requests and appeals involve individual requesters and/or involve

		agency records that contain PII. Each user's access is determined based on the user's role; for example: -Each OS FOIA Office Staff member and direct contractor has access to all or most records pertaining to the OS FOIA office and to requests referred to other FOIA offices; -Each OS FOIA Coordinator has access to only his/her program office's communications and records; -Each representative of another HHS FOIA office has access to only his/her FOIA office's requests and referral and report data; -A requester using PAL has access to only records pertaining to requests submitted through his/her PAL account; -System administrators have system-wide access but will only access PII if necessary to perform a system administrative task.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	User access is controlled by role-based access privileges, which are controlled by log-in credentials (for HHS users, which include employees and direct contractors, this is a PIV card and PIV PIN, plus a FOIAXpress user name and password; for PAL users, this is a user name and password).
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All such users are information disclosure specialists who use the system (or, in the case of the system contractor, designed the system) to process records for disclosure in accordance with FOIA and Privacy Act requirements. All such users receive initial and annual HHS IT system security and privacy awareness training. They also receive basic refresher training and advanced training on a regular basis at FOIA/Privacy Act training sessions and conferences/workshops hosted by HHS, the Department of Justice (DOJ) and outside vendors, regarding safeguarding personal privacy information and avoiding improper disclosures of PII.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Because such users are information disclosure specialists, they receive specialized training on a regular basis at FOIA/PA training sessions and conferences/workshops hosted by HHS, the Department of Justice (DOJ), and outside vendors providing advanced instructions and guidance regarding safeguarding personal privacy information and avoiding improper disclosures of PII in particular contexts and with respect to specific types of records.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The applicable records schedule is GRS 4.2, Information Access and Protection Records (formerly GRS 14); it prescribes retention periods ranging from approximately 2 years to 6 years after the date a case is closed. No records are permanently retained. The system is updated when a case is closed, calculates when case records are eligible for destruction, and generates a report of eligible cases each year, for use in deleting eligible electronic records and shredding eligible paper files. Disposition authority: DAA-GRS2016-0002-0001

PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative: User access is limited based on role and is controlled by log-in credentials (see next paragraph). Technical: Records stored in the system (which includes the Public Access Link (PAL)) are protected by encryption. Responsive records and communications containing PII are directly uploaded to the system from HHS users' encrypted workstation drives. HHS users (employees and direct contractors) must first log onto the HHS network with their PIV card and PIV PIN, using an HHS-issued laptop or personal computer (PC). HHS users who telework must access the system through HHS' virtual private network (VPN) using an HHS-issued laptop and their PIV card and PIV PIN. Members of the public who use PAL log into their PAL account with their user name and password. Separate web and database servers provide the online features used by requesters; each requester's access is limited to his/her PAL account. OS FOIA Office records are stored separately from records of other HHS FOIA Offices and records of other federal agencies that use FOIAXpress. Auditing features record when a user accesses the system and the actions taken. Physical: The buildings and offices where the system contractor's servers are located, and where HHS workstation laptops and PCs used to access the system are located, are secured by locks and security guards during off-duty hours, and by I.D. badges and security guards during office hours. Teleworkers' homes are secured by locks, and teleworkers use encrypted HHS laptops. Users do not leave computer screens unattended or visible to unauthorized persons.