Office of Justice Programs

Privacy Impact Assessment
for the
FOIAXpress

Issued by:
Maureen Henneberg

Approved by: Andrew J. McFarland
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: [February 20, 2025]

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Office of Justice Programs (OJP) utilizes a commercial web-based system called FOIAXpress to document and track the status of requests made by the public under both the Freedom of Information Act (FOIA) and the Privacy Act, store and process (redact) federal records maintained by OJP that are responsive to such requests, and generate both internal tracking reports and the annual and quarterly reporting statistics to the Department of Justice (DOJ). The system maintains personally identifiable information (PII) in the form of individual contact information necessary to respond to these requests and that may be contained within OJP's federal records that are responsive to specific FOIA and Privacy Act requests. The system includes the OJP Public Access Link (PAL), located at https://foiapal.ojp.usdoj.gov, which is a secure public-facing web portal that enables agencies to provide a centralized location for the public to submit FOIA requests.

FOIAXpress receives requests through the OJP PAL, the National FOIA Portal (FOIA.gov), or, in a relatively small number, via U.S. mail. FOIA.gov and PAL automatically populate requesters' contact information and requests into FOIAXpress, while authorized OJP users manually enter the contact information and requests into FOAIXpress for requests received via U.S. mail. The type of contact information included in the system depends on the contact information provided by the requester, but at minimum must include: (1) requester's name and (2) an email, work, or home address. In addition, the following contact information is entered, if provided by a requester: (1) mobile, work, and home phone numbers; (2) facsimile number; (3) organization; and (4) job title.

All records maintained by OJP that are responsive to a request are uploaded into the FOIAXpress by authorized OJP users, with responses to requesters completed outside the application. Responsive records stored within FOIAXpress may include PII prior to redactions; examples include, but are not necessarily limited to, human resources records related to federal personnel; federal grant applicant, recipient, and key personnel names and contact information; email communications include federal employee contact information and third-party names and contact information; and medical records related to the processing of Public Safety Officers' Benefits claims.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

FOIAXpress assists OJP in meeting its responsibilities under the FOIA by providing a platform that houses all the records associated with the processing of a request. The application also assists OJP with managing the FOIA case workload, by providing not only response timelines for requests, but request summary information on the disposition, pages reviewed, and exemptions applied.

FOIAXpress houses the administrative record for each FOIA and Privacy Act request received by OJP and enables authorized OJP users to process (review and redact) the federal records that are responsive to each request. The administrative record documents how a request was processed and includes: (1) the original FOIA or Privacy Act request; (2) any correspondence with the requester; (3) emails to OJP employees requesting a search for records responsive to the request; (4) all responsive records to the request, both original and redacted; and (5)

administrative forms documenting the OJP's processing of the request.

Only authorized users within OJP have access to the information compiled and records stored in the system. Information is either automatically entered into FOIAXpress through FOIA.gov or PAL or is manually entered or uploaded into the system by an authorized OJP user. Request data may be retrieved by searching requester name, email address, or FOIA or Privacy Act reference number. In most cases, OJP searches by the requester's name or request reference number.

FOIAXpress data fields are not customizable, and most are checkboxes to document receipt and closure dates and FOIA/Privacy Act exemptions applied to redact PII and other information that is statutorily exempt from disclosure. The only free text field is the request description field, which is either automatically populated by FOIA.gov or PAL or manually by authorized OJP users in the case of requests submitted via U.S. mail.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	The Freedom of Information Act (FOIA), 5 U.S.C. § 552 and the Privacy Act, 5 U.S.C. § 552a(d); 28 U.S.C. § 530C; 34 USC 10102; 5 U.S.C. §§ 552 and 552a .
Executive Order	
Federal regulation	Production or Disclosure of Material or Information, 28 C.F.R. Part 16
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	The name of requester, along with other individuals cited in the FOIA/PA request, or names of federal employees or third parties included in federal records responsive to a specific request.
Date of birth or age	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Place of birth	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Sex	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Race, ethnicity, or citizenship	X	C and D	Citizenship information is only requested for PA requests, or the information is included in federal records responsive to a specific request.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, and C	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Tax Identification Number (TIN)	X	A, B, C, and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Driver's license	X	A, B, C, and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, and D	This information is required only if the requester wishes to receive a response via U.S. mail or the information is included in federal records responsive to a specific request.
Personal e-mail address	X	A, B, C, and D	This information is required only if the requester wishes to receive a response via email or the information is included in federal records responsive to a specific request.
Personal phone number	X	A, B, C, and D	Only if the requester voluntarily provides it (or mobile number) in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Medical records number			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Medical notes or other medical or health information	X	A, C, and D	Only if federal records responsive to a specific request include federal employee or Public Safety Officers' Benefits program medical/health information.
Financial account information	X	A, C, and D	Only if federal records responsive to a specific request include federal employee or federal grant applicant or recipient financial account information.
Applicant information	X	C and D	Only if federal records responsive to a specific request include federal grant applicant information.
Education records	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Military status or other information	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Employment status, history, or similar information	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request or the information is included in federal records responsive to a specific request.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A	Only if the information is included in federal records responsive to a specific request.
Certificates	X	A, C, and D	Only if the information is included in federal records responsive to a specific request.
Legal documents	X	A, C, and D	Only if the information is included in federal records responsive to a specific request.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A and C	Only if the information is included in federal records responsive to a specific request.
Whistleblower, e.g., tip, complaint, or referral	X	A and C	Only if the information is included in federal records responsive to a specific request.
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			Only if the information is included in federal records responsive to a specific request.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Procurement/contracting records	X	A and C	Only if the information is included in federal records responsive to a specific request.
Proprietary or business information	X	A and C	Only if the information is included in federal records responsive to a specific request.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**			
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):			

3.1 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X

State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Other (specify): Private sector entities include law firms acting on behalf of requestors, educational institutions, and news agencies.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			OJP may share the information collected in FOIAXpress on a case-by-case basis, after a line-by-line review to redact all information exempt from disclosure, in order to respond to a FOIA or Privacy Act request. Information is shared on a need-to-know basis only.
DOJ Components	X			OJP may refer the records responsive to a FOIA or Privacy Act request to another DOJ component if the records originated with the other component for its direct response to the requester. Similarly, OJP may consult with another component to determine the appropriate response to a request if the responsive records contain equities belonging to the other component. OJP may route a misdirected request to another

				component if it is determined that the other component is the entity the requester intended to send the request. In these situations, OJP shares the general personal data and work-related data required to respond to the request. In addition, information is shared with United States Attorneys' Offices and the Civil Division if the request becomes the subject of litigation.
Federal entities	X			OJP may refer the records responsive to a FOIA or Privacy Act request to another federal agency if the records originated with the other agency for its direct response to the requester. Similarly, OJP may consult with another federal agency to determine the appropriate response to a request if the responsive records contain equities belonging to the other agency. OJP may route a misdirected request to another agency if it is determined that the other component is the entity the requester intended to send the request. In these situations, OJP shares the general personal data and work-related data required to respond to the request.
State, local, tribal gov't entities	X			OJP may provide records responsive to FOIA/PA requests to OJP from these entities, after a line-by-line review to redact all information exempt from disclosure.
Public	X			OJP may share the information collected in FOIAXpress on a case-by-case basis, after a line-by-line review to redact all information exempt from disclosure, in order to respond to a FOIA or Privacy Act request.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			OJP may share the information collected in FOIAXpress on a case-by-case basis, after a line-by-line review to redact all information exempt from disclosure, in order to respond to FOIA or Privacy Act litigation.
Private sector	X			OJP may provide records responsive

				to FOIA/PA requests to OJP from the private sector, after a line-by-line review to redact all information exempt from disclosure.
Foreign governments	X			OJP may provide records responsive to FOIA requests from foreign governments, after a line-by-line review to redact all information exempt from disclosure.
Foreign entities	X			OJP may provide records responsive to FOIA requests from foreign entities, after a line-by-line review to redact all information exempt from disclosure,
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The information in this system will not be released for "open data" purposes. It is used to generate the annual and quarterly reporting statistics to OIP as required by FOIA. The reports only include statistical data on the processing of requests – there is no PII included in the statistical data or the reports.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

FOIAXpress is covered under JUSTICE/DOJ-004, "Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records"; 77 FR 26580 (May 4, 2012); 82 FR 24151, 152 (May 25, 2017); and Exemptions Claimed Pursuant to 5 U.S.C. 552a(j) and (k). See 28 C.F.R. § 16.130.

System access, administration, and audit information for FOIAXpress are covered by JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 37188 (Jul. 14, 2021).

FOIAXpress receives submissions through FOIA.gov and PAL, or through manual entries by authorized OJP users for the relatively small number of requests received via U.S. mail. The following notice is provided to individuals who visit OJP's PAL website: https://www.justice.gov/doj/privacy-policy.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

In terms of collection of information, individuals are not required to submit Privacy Act or FOIA requests to the Department, and even where individuals do submit requests, they may decline to provide any additional requested information. However, OJP will be unable to respond to any request that does not provide sufficient information to process the request. Similarly, a person seeking records under the Privacy Act who does not provide adequate identifying information under 28 C.F.R. § 16.41(d), will only receive information under the FOIA.

Individuals do not have an opportunity to consent to particular uses of the information because the FOIA and Privacy Act both govern the federal government's obligation to provide the public access to federal records, subject to specific statutory exemptions for the redaction of information (including PII in most circumstances) prior to release.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals seeking copies of information pertaining to them maintained within FOIAXpress may submit a Privacy Act request. As provided in the Mandatory Declassification Review Records System of Records Notice, individuals seeking to contest or amend records must directly contact the applicable DOJ component office. Consistent with 28 C.F.R. Subpart D §16.46, all requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls.** **Provide date of most recent Authorization to Operate (ATO):** Issued: 12/15/2023; Expires: 12/15/2026 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** **FOIAXpress is categorized as a Moderate risk system. This categorization is based on universal categorization of Moderate assessments in Confidentiality, Integrity, and Availability for both its Personal Identity and Authentication as well as its Official Information Dissemination Information Types.**
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** **FOIAXpress is subject to an annual internal assessment of OJP's defined Core Controls conducted throughout the course of the Fiscal Year.**
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** **OJP is responsible for application-level logging, where all other logging is under the purview of the SaaS solution, AINS eCase. FOIAXpress can audit (i) logon attempts; (ii) account management; (iii) successful/unsuccessful access; (iv) policy and configuration changes; (v) system level access; (vi) process tracking and system events; and (vii) all activities pertaining to web apps.**
	Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The ITSD Account Management team monitors the use of information system accounts. System Owners notify Account Managers when accounts are no longer required, terminated, or transferred, and an individual's system usage or need-to-know status changes. Authorizing access to information systems is based on valid access authorization, intended system use and other attributes as required by OJP. System Owners review accounts for compliance with account management requirements annually. OJP users authenticate through the OJP ADFS domain and Multi-factor PIV authentication is enforced.

OJP has implemented physical and logical security controls that comply with department standards and policies regarding protection of sensitive information in digital and non-digital form. FOIAXpress adheres either directly or through inherited hybrid controls the suite of Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), Risk Assessment (RA), System and Communications Protection (SC), and System and Information Integrity (SI). Of these, the implemented controls are as follows:

- Per AC-5 and AC-6: Least Privilege, employs four user groups (Admin, FOIA Officer, Intake, Legal Review and Processors) whose functions are distributed and separated based on belonging to any one of four applications (Action Office Manager FOIA Officer, User, ADR Roles, All Access, Intake, Processors, Correspondence Template - Edit, and Legal Review).
- FOIAXpress inherits some identity and access management (IAM) functions from its proprietary DIAMD tool, which manages internal accounts in compliance with OCIO 30, while AINS eCASE manages external accounts. Per AC-2(12), the system is monitored for atypical activity.
- FOIAXpress employs hybrid implementation of AU-2: Event Logging, and AU-6: Audit Record Review, Analysis, and Reporting between OJP's internal audit review and remediation capability as well as that of AINS for its eCase system.
- AU-2 ensures that logging SIEMs can detect logon attempts, successful/unsuccessful access, system level access, process tracking, and system events.
- Per SC-7(8), all internal traffic bound for external networks is sent through authenticated proxy servers within the managed interfaces of boundary protection devices.
- The system's System and Information Integrity family of controls are wholly inherited from the DOJ Common Controls Program.

All of the above controls, in addition to others that do not immediately pertain to minimization of privacy risks, are reviewed annually as part of OJP's internal Core Control assessment and are tested based on the most current artifacts available to the ISSO and the system team. Furthermore, FOIAXpress is FISMA reportable, which makes it potentially subject to a FISMA audit when certain systems are selected for audit every three years. It is also potentially subject to OMB's A-123 Audit, which includes the SC and SI family of controls among its 29 audited Determine If Statements (DISes).

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records maintained in FOIAXpress are retained and disposed of in accordance with records retention schedules approved by the National Archives and Records Administration. NARA's General Records Schedule (GRS) 4.2, Information Access and Protection Records, controls the retention and destruction of records pertaining to information service functions performed by agencies, including the FOIA, Privacy Act, and Mandatory Declassification Review (MDR) files. Under GRS 4.2, agencies may retain FOIA, Privacy Act, and MDR records for a maximum of six years after final agency action, and litigation records for a maximum of three years after final adjudication by the courts, whichever is later, unless a business use authorizes longer record retention.

FOIAXpress contains an internal management feature that categorizes information based on the

appropriate records retention schedule. When the retention period ends for a particular piece of information, the system alerts the administrator that the retention period has ended. At that time, the system administrator can authorize deletion of the information.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ____X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

FOIAXpress is covered by the: Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records SORN, DOJ-004, last published in full at 77 Fed. Reg. 26580 (May 4, 2012) with exemptions claimed pursuant to 5 U.S.C. 552a(j) and (k). See 28 C.F.R. § 16.130.

System access, administration, and audit information for FOIAXpress are covered by JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

FOIAXpress benefits the Department by allowing OJP to receive and process FOIA and Privacy Act requests. In order to respond to requests from the public, OJP must collect information corresponding to a requester concerning the requester's FOIA request or Privacy Act request. For Privacy Act requests, the information collected is also used to verify the requester's identity before releasing information. As for the records processed through FOIAXpress, these are records that were already in the possession of the Department prior to the request. OJP minimizes the privacy risk of storing and disseminating more PII than is necessary by communicating with requesters and providing them with an opportunity to narrow the scope of their request. This risk is also mitigated by adhering to NARA's guidelines and record retention policies.

All authorized OJP FOIAXpress users are responsible for protecting the privacy rights of both requesters and individuals whose PII may be contained in OJP records that are responsive to specific request. In order to mitigate the privacy risk from unauthorized disclosure and sharing of PII outside the Department, authorized OJP users are trained on the statutory exemptions to disclosure, including the exemptions specific to the identification of and protection of PII, as well as the FOIAXpress redaction processes and procedures to prevent the unauthorized disclosure of information. Staff redact

information that is exempt from disclosure pursuant to statutory exemptions from responsive federal records prior to disclosing them to the requestor. Additionally, staff members must take annual OPCL Privacy Act and Cyber Security Awareness Training and sign the DOJ Rules of Behavior.

OJP may share the information collected in FOIAXpress on a case-by-case basis in order to respond to a request. For example, if OJP locates records in response to a request in which another agency or component has an interest, OJP may consult with the other agency/component before making a release determination, or OJP may refer those records to the other agency/component for direct response to the requester. OJP would share the requester's contact information with the other agency to facilitate their direct response to the requester. When shared within the Department, other components are required to conform to Department policies to prevent or mitigate threats to privacy through disclosure, such as maintaining the integrity of their FOIA tracking application.