Community Oriented Policing Services (COPS Office)

Privacy Impact Assessment
for:

FOIAXpress

Issued by:

Melissa Fieri-Fetrow, Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [March 5, 2021]

(May 2019 DOJ PIA Template)

This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The COPS Office utilizes a commercial off-the-shelf web-based system called FOIAXpress. FOIAXpress is used to document and track the status of requests made by the public under both the Freedom of Information Act (FOIA) and the Privacy Act for documents maintained by the COPS Office, and to generate the annual and quarterly reporting statistics to the Department of Justice (DOJ) as required by FOIA. The system maintains individual contact information necessary to respond to these matters.

FOIAXpress does not collect information directly from individuals, their representatives, or from other DOJ components and other federal entities. Only the requester's contact information and a description of the request are entered into the system. 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; and (3) job title.

All records related to a request are uploaded into the FOIAXpress. The type of records uploaded include: (1) the original FOIA request; (2) any correspondence with the requester; (3) emails to COPS 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 COPS Office's processing of the request.

Only approved users within the COPS Office have access to the information compiled in the system. Information is entered into the system by an approved COPS Office user and may be retrieved by searching requester name, email address, or FOIA reference number. In most cases, the COPS Office searches by the requester's name or FOIA reference number. The records maintained in FOIAXpress depends on the information the requester provides via mail or email and the office records responsive to the request. In addition, FOIAXpress data fields are not customizable and most are checkboxes to document receipt and closure dates and FOIA exemptions applied. The only free text field is the request description field.

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.

The purpose of FOIAXpress is to house the administrative record for each FOIA request received by the COPS Office. The administrative record documents how a request was processed and includes: (1) the original FOIA request; (2) any correspondence with the requester; (3) emails to COPS 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 COPS Office's processing of the request.

All records are uploaded into FOIAXpress, with responses to requesters and the redaction of records completed outside the application. Although FOIAXpress does not collect any information, it assists the COPS Office 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 functions assist the COPS Office 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.

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)
	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

3.1 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	C and D	The name of requester, along with other individuals cited in the FOIA/PA request.
Date of birth or age	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Place of birth	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Gender	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Race, ethnicity or citizenship	X	C and D	Citizenship information is only requested for PA requests.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Tax Identification Number (TIN)	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Driver's license	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	This information is required only if the requester wishes to receive a response via U.S. mail.
Personal e-mail address	X	C and D	This information is required only if the requester wishes to receive a response via email.

Personal phone number	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request. Mobile phone numbers are also collected if the requester provides them in the FOIA/PA request.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Military status or other information	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Employment status, history, or similar information	X	C and D	Only if the requester voluntarily provides it in the FOIA/PA request.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			

(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
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			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact Information			
Procurement/contracting records			
Proprietary or business information			

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:			The system's audit log compiles the date and time of each user's access and the files the user accessed. User ID's are maintained as part of each user's profile and may only be edited by a system administrator.
- User ID	X	A	
- User passwords/codes	X	A	
- IP address			
- Date/time of access	X	A	
- Queries run	X	A	
- Content of files accessed/reviewed	X	A	
- Contents of files	X	A	
Other (please list the type of info and describe as completely as possible):			

3.2 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	
Phone		Email	X		

Other (specify):

If an attorney represents an individual, the attorney may provide information on the client's behalf. Because the attorney acts as the client's representative, the COPS Office considers any personal information provided by an attorney as submitted by the individual client.

Government sources:					
Within the Component		Other DOJ Components	X	Online	

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

Other (specify):
When a request received by the COPS Office requires records held by another DOJ component or federal agency, the COPS Office may reach out to that component or agency for the responsive records. In that case, information from other DOJ components or federal records may be collected and maintained within FOIAXpress.

Similarly, when another DOJ component or federal agency receives a request for records held by the COPS Office, that other component or agency may either request responsive records from the COPS Office or refer that request to the COPS Office for handling. In that case, COPS (via FOIAXpress) maintains that request, as well as whatever general personal and work-related data about the requester is necessary to obtain the responsive records.

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					

Other (specify):

All records are uploaded into FOIAXpress, the application does not solicit information from requesters. The only information needed from a requester is contact information and a description of the records being requested. FOIAXpress maintains general personal data and work-related data provided by a requester pursuant to a FOIA or Privacy Act request.

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			The COPS Office may share the information collected in FOIAXpress on a case-by-case basis in order to respond to a FOIA or Privacy Act request. Information is shared on a need-to-know basis only.

DOJ Components	X			The COPS Office 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, the COPS Office may consult with another component to determine the appropriate response to a request if the responsive records contain equities belonging to the other component. The COPS Office 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, the COPS Office shares the general personal data and work-related data required to respond to the request. Information may be shared with OIP if the request is the subject of an administrative appeal. 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			The COPS Office 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, the COPS Office may consult with another agency to determine the appropriate response to a request if the responsive records contain equities belonging to the other agency. The COPS Office 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, the COPS Office shares the general personal data and work-related data required to respond to the request.

State, local, tribal gov't entities				
Public	X			The COPS Office may share the information collected in FOIAXpress on a case-by-case basis in order to respond to a FOIA or Privacy Act request.

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			The COPS Office may share the information collected in FOIAXpress on a case-by-case basis in order to respond to FOIA or Privacy Act litigation.
Private sector				
Foreign governments				
Foreign entities				
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.

This system 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 request, no personally identifiable information is included in 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.

FOIAXpress does not collect information directly from requesters.

The following notice is provided to individuals who visit the COPS Office 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.

Records are only uploaded into FOIAXpress, the application does not collect or solicit information from requesters.

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, the COPS Office 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. However, the information maintained in FOIAXpress is not disclosed to any third party without the advance written consent of the person to whom the records pertain, unless one of twelve exceptions which permit disclosure without the consent of the individual of record applies. See 5 U.S.C. §552(a)b, .

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.

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 CFR 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):** October 1, 2019 **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:** There are no open POAMs for FOIAXpress.
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** FOIAXpress has measures in place to appropriately safeguard information uploaded by COPS to their platform. Support services are provided by AINS, a leading global provider of cloud-based, adaptive case management platforms and solutions for government and commercial markets. The services provided by AINS support the use of their FOIAXpress application in accordance to FedRamp, and FISMA requirements, including providing DR site, regular backups, physical controls to meet FedRAMP compliance, application security, audit logs.
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:** The system's audit log compiles the date and time of each user's access and the files the user accessed. AINS checks the logs every week and also get schedule reports from audit log tool for pre-defined events. User ID's are maintained as part of each user's profile and may only be edited by a system administrator.
X	**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**.
X	**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?

FOIAXpress uses role-based permissions to control a user's access to information in the application. The authentication controls require each user to utilize a user name and password. Password controls prompt users to create a new password on a regular basis and require the user to create a strong password. The role-based access controls allow the system administrator to grant access to information based on a least privilege access setting. Staff members must also take annual OPCL Privacy Act and Cyber Security Awareness Training and sign the DOJ Rules of Behavior.

A FOIAXpress administrator can run user audit reports in FOIAXpress regarding what users have accessed, added, downloaded or deleted information from the system. Data is encrypted in transit and at rest using Federal Information Processing Standards (FIPS) and Transport Layer Security (TLS) protocols that meet NIST standards.

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 (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.

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?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Potential Threats Related to Information Collection

The information housed in FOIAXpress is required for the COPS Office to process FOIA and Privacy Act requests for records received by the office. In order to respond to requests from the public, the COPS Office must collect information to correspond with 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.

Records maintained in FOIAXpress are retained and disposed of in accordance with record 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.

b. Potential Threats Related to Use of the Information

The FOIAXpress application is hosted in a FedRAMP moderate facility, and access to the servers is on a need-to-know basis by cleared staff. FOIAXpress employs authentication and role-based access controls to ensure data is handled, retained, and disposed of appropriately. The authentication controls require each user to utilize a user name and password. Password controls prompt users to create a new password on a regular basis and require the user to create a strong password. The role-based access controls allow the system administrator to grant access to information based on a least privilege access setting.

FOIAXpress system management contractors have access to data for system maintenance and enhancement. All users are responsible for protecting the privacy rights of requesters and receiving appropriate training. Additionally, COPS Office staff are trained on redaction processes and

procedures to prevent the unauthorized disclosure of information. Staff redact sensitive information from all documentation prior to disclosing. Additionally, staff members must take annual OPCL Privacy Act and Cyber Security Awareness Training and sign the DOJ Rules of Behavior.

c. Potential Threats Related to Dissemination

The COPS Office may share the information collected in FOIAXpress on a case-by-case basis in order to respond to a request. For example, if the COPS Office locates records in response to a request in which another agency or component has an interest, the COPS Office may consult with the other agency/component before making a release determination, or the COPS Office may refer those records to the other agency/component for direct response to the requester. The COPS Office would share the requester's contact information with the other agency to facilitate their direct response to the requester.

The COPS Office shares information on a need-to-know basis only, and may share information via email, mail, facsimile, or phone in accordance with Department policies. 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.