Drug Enforcement Administration

Privacy Impact Assessment
for FOIAXpress

Issued by:
David J. Mudd
Senior Component Official for Privacy
Drug Enforcement Administration

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

Date approved: September 30, 2022

(May 2019 DOJ PIA Template)

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 FOIAXpress is a web-based application that the Drug Enforcement Administration's (DEA) Freedom of Information and Privacy Act Unit (CCAR) uses to process all Freedom of Information Act and Privacy Act (collectively "FOIA") requests to DEA. CCAR uses FOIAXpress to track and fulfill requests seeking access to non-public DEA records, as well as to store and manage copies of records gathered in response to FOIA requests that can contain personally identifiable information (PII) about a requester or other individuals mentioned or discussed in the records. Given the nature and types of information contained in FOIAXpress, the Privacy Impact Assessment (PIA) was conducted to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; specifically, to determine the risks and effects of collecting, maintaining, and disseminating such information in FOIAXpress, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA helps to ensure that privacy protections are built into FOIAXpress from the start, allowing to safeguard both the information collected and the viability of the project.

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.

CCAR is responsible for processing all FOIA requests submitted to DEA. In performing this function, FSR utilizes FOIAXpress – a web-based commercial off-the-shelf application owned and maintained by AINS Inc. FSR uses FOIAXpress to track and fulfill requests filed by members of the public seeking access to non-public DEA records both under the FOIA and Privacy Act (PA). The FOIAXpress system is accessible through DEA's Firebird information management single sign-on utilizing the Personal Identity Verification (PIV) card for user identification and access control. System access is restricted to the CCAR staff solely by use of a separate assigned user ID and password-protected entrance access to FOIAXpress through a secure website available only on the DEA network. The system allows CCAR staff to log and track the processing of each FOIA request. The system records the status of the request, relevant deadlines, and other key events or data, such as the dates that actions occurred. The system also stores internal and external correspondence, such as memoranda to supervisors, requests for records sent to staff, communications with requesters, and other data entered by CCAR staff. The CCAR also uses FOIAXpress to store and manage copies of the non-public agency records that have been gathered in response to requests. These copies can contain PII about a requester or other individuals mentioned or discussed in the records.

Professionals within CCAR have access to the records as necessary to perform administrative functions (e.g. create requester profiles, log incoming FOIA requests), prepare responses to FOIA requests, and to prepare periodic reports as required by law, executive order, or agency directive. System users may share information maintained within the system (e.g., requester contact information, PII existing within responsive records) with DOJ and other DEA staff, including FOIA/PA liaisons and records custodians, as necessary to search for and to appropriately review and redact responsive records prior to their release. DEA's Information Systems Division, the Office of Chief Counsel, Administrative/General Law Section (CCA), and paralegal contractors in CCAR have access to administer and support FOIAXpress operations as necessary.

In most cases, CCAR searches by the request number assigned to the case. CCAR may also search using other identifiers, such as the requester's name, description, or date of the request. Although FOIAXpress is a web-based application, members of the public such as requesters do not have any access to the system. Requesters may submit requests by mail or email. CCAR manually enters the request information into FOIAXpress for tracking. CCAR provides responses to the requester via mail or email, depending on the requester's preference.

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
X	Statute	5 U.S.C. § 301 and 44 U.S.C. § 3101 to implement the provisions of 5 U.S.C. § 552 and 5 U.S.C. § 552a
	Executive Order	
	Federal Regulation	
	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
Name	X	A, B, C and D	Names to include aliases, of Federal Government employees and members of public (USPERs and non-USPERs)
Date of birth or age	X	A, B, C and D	DOB and age of Federal Government employees and members of public (USPERs and non-USPERs)
Place of birth	X	A, B, C and D	POB of Federal Government employees and members of public (USPERs and non-USPERs)
Gender	X	A, B, C and D	Gender of Federal Government employees and members of public (USPERs and non-USPERs)
Race, ethnicity or citizenship	X	A, B, C, and D	Race, ethnicity or citizenship of Federal Government employees and members of Public (USPERs and non-USPERs)
Religion	X	A, B, C, and D	Although the system does not specifically ask for such information, Religion may be contained in FOIA/PA requests and responsive documents for Federal Government employees and members of public (USPERs and non-USPERs).
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Full SSN of Federal Government employees and members of public (USPERs and non-USPERs), voluntarily provided
Tax Identification Number (TIN)	X	A, B, C and D	TIN of Federal Government employees and members of public (USPERs and non-USPERs)
Driver's license	X	A, B, C and D	Driver's license of Federal Government employees and members of public (USPERs and non-USPERs)
Alien registration number	X	C and D	A-number of members of public (USPERs and non-USPERs), voluntarily provided
Passport number	X	A, B, C and D	Passport numbers of Federal Government employees and members of public (USPERs and non-USPERs)

(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
Mother's maiden name	X	A, B, C, and D	Mother's maiden name of Federal Government employees and members of public (USPERs and non-USPERs)
Vehicle identifiers	X	C and D	VINs of vehicles of members of public (USPERs and non-USPERs)
Personal mailing address	X	A, B, C and D	Mailing addresses of Federal Government employees and members of public (USPERs and non-USPERs)
Personal e-mail address	X	A, B, C, and D	E-mail addresses of Federal Government employees and members of public (USPERs and non-USPERs)
Personal phone number	X	A, B, C and D	Phone numbers of Federal Government employees and members of public (USPERs and non-USPERs)
Medical records number	X	A	DEA employees' medical records that contain such number
Medical notes or other medical or health information	X	A	DEA employees' medical records
Financial account information	X	A, B, C, and D	Financial accounts and partial credit card information of Federal Government employees and members of public (USPERs and non-USPERs)
Applicant information	X	A, B and C	Information about applicants for employment with DEA from DOJ and its components, other Federal employees, and members of public (USPERs)
Education records	X	A, B, C, and D	Education records of DEA and other Federal Government employees and members of public (USPER and non-USPERs)
Military status or other information	X	A, B, C, and D	Although the system does not specifically ask for such information, military status or similar information may nonetheless be included in FOIA/PA requests and responsive documents for Federal Government employees and members of public (USPERs and non-USPERs).

(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
Employment status, history, or similar information	X	A, B, and C	Employment related information of DEA and other Federal Government employees' and members of public (USPERs)
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, and C	Information related to performance of DEA and other Federal Government employees and members of public
Certificates	X	A, B, C, and D	Certificates and licenses, of DEA and other Federal Government employees related to their employment. or of members of the public (USPERs or non-USPERs) necessary to deal with Substance Control Act
Legal documents	X	A, B, C, and D	Legal documents related to civil lawsuits against DEA and other Federal employees, or alleged criminal acts of DEA and other Federal Government employees or members of public (USPERs and non-USPERs)
Device identifiers, e.g., mobile devices	X	C and D	Model and serial numbers of electronic devices of members of public (USPERs and non-USPERs) ceased as evidence for law enforcement purposes
Web uniform resource locator(s)	X	A, B, C, and D	Although the system does not specifically ask for such information, web uniform resource locator(s) may nonetheless be included in some FOIA/PA requests or responsive documents for Federal Government employees and members of public (USPERs and non-USPERs).
Foreign activities	X	A, B, C and D	Investigative records collected in response to FOIA requests that contain information about activities that took place in foreign states for Federal Government employees or members of public (USPERs and non-USPERs).

(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	X	A, B, C, and D	Criminal records of Federal Government employees and members of public (USPERs and non-USPERs) and information about employment related civil lawsuits against DEA or its employees
Juvenile criminal records information	X	C and D	Criminal records of members of public (USPERs and non-USPERs)
Civil law enforcement information, e.g., allegations of civil law violations	X	A, C, and D	Information about employment related civil lawsuits against DEA by members of the public (USPERs and non-USPERs). or its employees.
Whistleblower, e.g., tip, complaint or referral	X	A	Complaints filed by DEA employees
Grand jury information	X	A, B, C, and D	Investigative records compiled for prosecution of DEA or other Federal Government employees or members of public (USPERs and non-USPERs) alleged to have committed criminal acts
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	Information concerning witnesses to criminal matters, such as, witness name and contact information, witness statements, etc., compiled for prosecution of DEA or other Federal employees or members of public (USPERs and non-USPERs) alleged to have committed criminal acts
Procurement/contracting records	X	A, C, and D	Records of DEA contacting obtained in response to FOIA requests
Proprietary or business information	X	A, B, C, and D	Names, property and email addresses and other identifying information of business of Federal Government employees and members of public (USPERs and non-USPERs)

(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
Location information, including continuous or intermittent location tracking capabilities	X	C and D	Location and other similar information obtained using tracking capabilities contained in records responsive to FOIA requests from members of public (USPERs and non-USPERs)
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Photos of DEA and other Federal employees or members of public (USPERs and non-USPERs)
- **Video containing biometric data**	X	A, B, C, and D	Biometrics data of DEA and other Federal employees or members of public (USPERs and non-USPERs)
- **Fingerprints**	X	A, B, C and D	Fingerprints of DEA and other Federal employees or members of public (USPERs and non-USPERs)
- **Palm prints**	X	A, B, C and D	Although the system does not specifically ask for such information, palm prints may nonetheless be included in responsive documents for Federal employees and members of public (USPERs and non-USPERs).
- **Iris image**	X	C and D	Although the system does not specifically ask for such information, iris images may nonetheless be included in responsive documents for members of public (USPERs and non-USPERs).
- **Dental profile**	X	C and D	Although the system does not specifically ask for such information, dental records may nonetheless be included in responsive documents for members of the public (USPERs and non-USPERs)..
- **Voice recording/signatures**	X	A, B, C, and D	Voice recording/signatures of DEA and other Federal employees or members of public (USPERs and non-USPERs)
- **Scars, marks, tattoos**	X	C and D	Scars, marks, tattoos or other identifiable information of members of public (USPERs and non-USPERs) contained in individual files

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	C and D	Although the system does not specifically ask for such information, DNA profiles may nonetheless be included in responsive documents.
Other (specify)	X	A, B, C and D	Request Number assigned to the FOIA case of Federal Government employees and members of public (USPERs and non-USPERs)
System admin/audit data:			
- **User ID**	X	A	System audit related information e.g. user ID of DEA employees and contractors
- **User passwords/codes**	X	A	System audit related information e.g. passwords of DEA employees and contractors
- **IP address**	X	A	System audit related information e.g. I.P. address of DEA employees and contractors.
- **Date/time of access**	X	A	System audit related information e.g. date/time of access of DEA employees and contractors.
- **Queries run**	X	A, C and D	NADDIS and NCIC report search on members of public (USPERs and Non-USPERs). Also names of DEA employees who inquire and search for responsive records within DEA offices
- **Content of files accessed/reviewed**	X	A and B	Information about Federal Government employee who have accessed/ reviewed files, as well as the dates, times and contents of the files that were accessed/reviewed
- **Contents of files**	X	A, B, C, and D	Any information contained in FOIA request case files

(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
Other (please list the type of info and describe as completely as possible):	X	A, B , C and D	Possible instances of unknown PII related information could be collected when a death certificate accompanies the FOIA request for employees, contractors, other federal government personnel, members of the public (US or non-USPERs); and/or Prescriber ID's of members of the public (US or non-USPERs); could also be collected.

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	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
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): 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			CCAR shares certain information within the DEA offices and other DEA staff, including FOIA/PA liaisons and records custodians, as necessary to search and locate records responsive to FOIA requests submitted to DEA.
DOJ Components	X			System users may share information maintained within the system (e.g. requester contact information, PII existing within responsive records) with any DOJ component as necessary to search and locate records responsive to FOIA requests submitted to DEA, and address DOJ questions related to FOIA appeals.
Federal entities	X			CCAR may share PA records with any federal entities under routine-use sharing provision of the PA.
State, local, tribal gov't entities	X			CCAR may share with any state, local or other government entities records requested and covered under SORNs that have a routine-use sharing provision.
Public	X			To fulfill its obligations under both the FOIA and the PA, CCAR disseminates only records that were responsive to requesters' FOIA/PA requests and were collected, stored, reviewed, and maintained in FOIAXpress in response to said requests.

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			Counsels and other parties to litigation may make FOIA/PA requests, and CCAR will provide records responsive to the requests as required under the FOIA and the PA. Additionally, in certain instances, CCAR searches and provides DEA records responsive to courts' orders requesting such records.
Private sector	X			CCAR will provide records responsive to FOIA/PA requests to DEA from the private sector.
Foreign governments	X			CCAR will provide records responsive to FOIA requests from foreign governments.
Foreign entities	X			CCAR will provide records responsive to FOIA requests from 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.

CCAR does not release information to the public for "Open Data" purposes. However, under the FOIA, specifically Subsection (a)(2) of the Act, DEA is required to make available for public inspection in an electronic format certain records that have been requested and released under the FOIA three or more times – which typically is accomplished by posting on DEA's publicly available website. The records disclosed under the subsection are related to DEA, such as specific policy statements, certain administrative staff manuals, and instructions to staff. While such records generally do not include PII, prior to making them public, the records are reviewed, and any PII and sensitive information is appropriately redacted to ensure privacy protection.

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.

Notice is provided to individuals by both (e)(3) statements and a SORN. FOIAXpress may maintain information about the individual—such as name, alias, home address, telephone number, email address, DOB, social security numbers (SSN), etc.—seeking access to information under the FOIA or the Privacy Act (PA). As such, requesters provide their contact information and, for requesters seeking information about themselves under PA, a certification of identity form (DOJ 361) as required by Department of Justice regulations. The DOJ-361 form contains a Privacy Act § 552a(e)(3) notice for individuals submitting the form. The form expressly states the principal purpose and the authority for solicitation of the information, that the disclosure of the SSN is optional, and the consequences of not furnishing certain information.

Moreover, the Department of Justice (DOJ) system of records entitled "Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records (Justice/DOJ–004)," 77 Fed. Reg. 26580 (May 4, 2012), last published at 82 Fed. Reg. 24151, 152 (May 25, 2017), provides general notice to the public about the collection, use, and sharing of individuals' PII; namely, that it is necessary for processing their access, access and amendment, requests under the FOIA and the PA respectively.

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.

FOIAXpress does not specifically require the collection of PII or other information but rather maintains information about FOIA requesters who submit FOIA requests to DEA. FOIAXpress also maintains certain records collected in response to FOIA requests that may contain PII mentioned in those records. Thus, FOIA/PA requesters consensually furnish information, as required under the FOIA and PA, to gain, and to facilitate the process of gaining, access to records about themselves or others.

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.

DEA's public facing website contains a FOIA/PA webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. The website also contains procedures for filing a request for record correction or amendment to DEA.

FOIAXpress maintains records about FOIA/PA requests submitted to DEA. Access to these records is permitted under the PA and is also outlined in Justice/DOJ–004, *Privacy Act, and Mandatory Declassification Review Records*. Specifically, all requests for access to these records must be in writing and should be addressed to DEA's Freedom of Information and Privacy Act Unit (CCAR).

The request should include a general description of the records sought and must include the requester's full name, current address, date of birth, and place of birth. The request must be signed, dated and either notarized or submitted under penalty of perjury (i.e., DOJ-361 form).

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):** The ATO was granted on September 22, 2021 and has an expiration date of September 30, 2024. **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:** N/A, there are no outstanding POAMs for privacy related controls.
	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:** System utilized development, unit, pre-production, regression, and pilot testing as part of the ATO processes. Additionally, validation of the ATO artifacts and implementation of security requirements, such as Splunk auditing/monitoring, performed by DEA Cybersecurity Services.
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 application audit logs are reviewed daily as part of the Cybersecurity Operations, Response and Engineering Unit (TCVV) review process. The Operations & Response team reviews all logs forwarded from DEA systems for suspicious behavior and notifies the system owner/security points of contact of any alerts. Additionally, the program management office performs periodic reviews to ensure user and system behavior comply with all applicable DOJ, DEA, and federal guidelines, policies, and laws.
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**. Yes, as a standard operating procedure, all contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.

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:** DOJ's Office of Privacy and Civil Liberties travelled to HQ to conduct Privacy Act training for all FOIAXpress end users prior to application initiation in 2018. Additionally, Privacy Act training is conducted annually and throughout the year in order to provide an overview of agency employees' obligations to protect PII. The component has a requirement for all employees to include contract employees to complete the mandated Cyber Security Awareness Training annually.

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 is limited (by software licenses) to a small number of specified DEA employees who need system access to perform their duties. The NIST FIP status for FOIAXpress is Moderate. The FOIAXpress system is accessible through DEA's Firebird information management single sign-on utilizing PIV cards for user identification and access control. Furthermore, FOIAXpress requires an additional User ID and password protected entry point into the system for all users. Access to the system itself is protected and monitored by authentication controls, role-based access controls, and system auditing. The system also has the capacity to employ additional audit trail procedures about system users and to track activity on specific FOIA requests as necessary. FOIAXpress users must read and sign DEA's IT Rules of Behavior. Moreover, all users must complete annual DOJ security awareness training.

In addition to the above-stated protective measures, DEA buildings are guarded and monitored by security personnel, cameras, access badges with picture identification, and other physical security measures. Access to all electronic records within DEA is controlled by User ID and password combination and other electronic access (e.g., Personal Identification Verification card) or network access (e.g., firewalls).

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 are retained and disposed of in accordance with the National Archives and Records Administration's (NARA) General Records Schedule 4.2-020.

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:

JUSTICE/DOJ-004, "Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records," 77 Fed. Reg. 26580 (May 4, 2012), last published at 82 Fed. Reg. 24151, 152 (May 25, 2017).

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?

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the Department's official duties is always a potential threat to privacy. The CCAR utilizes FOIAXpress for the sole purpose of fulfilling its obligations under the FOIA and PA for processing all FOIA/PA requests submitted to DEA. As such, CCAR collects, stores, maintains, and shares only those records that have been collected in response to FOIA/PA requests. In an effort to reduce the collection of data, CCAR staff communicates with requesters, providing them the opportunity, and helping them to narrow the scope of their request. Any potentially responsive record is then searched, narrowing the scope of information maintained in FOIAXpress based on specific documents, search terms, date range, etc. To avoid the collection of unnecessary personal information, CCAR collects only from those sources of information that contain specific records responsive to FOIA/PA requests made. Additionally, records in FOIAXpress are retained and disposed of in accordance with the NARA's guidelines and schedule.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the Department's use of the information in the FOIAXpress system include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information.

To mitigate privacy risks associated with the collection, use, access, dissemination, and maintenance of the information in FOIAXpress, the system stores only records collected in response to FOIA requests submitted to DEA, and those records are shared only with individuals making those requests. Moreover, the access to the records contained in the system is strictly limited. Only a small number of

DEA employees and contractors, who are trained and knowledgeable of the IT Rules and Behavior and DOJ security measures, have access to FOIAXpress. The FOIAXpress system is accessible through DEA's Firebird information management single sign-on utilizing the Personal Identity Verification (PIV) card for user identification and access control. Furthermore, those permitted to use FOIAXpress are also required to have unique and personalized User ID and password protected entry into the system. The system also has the capacity to monitor the system users and to track their activities in the system. CCAR staff are also provided with annual training on the PA, and they ensure that all information DEA maintains on individuals is appropriately safeguarded. PA-protected information, that is, records responsive to FOIA/PA requests that contain any PII, is sent to requesters via encrypted e-mail.

c. Potential Threats Related to Dissemination

There is a potential risk to privacy that could result from improper access and the potential unauthorized disclosure of the information within the FOIAXpress system. However, security protections that authorize and limit a user's access to information within the system mitigate this risk. For example, consistent with FISMA and NIST security controls, transmissions of DEA non-public data, including those that potentially contain information responsive to FOIA requests, occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), Secure Sockets Layer (SSL), or other encryption.

Another privacy risk related to dissemination is disclosure to persons without authority to receive the information. The DEA mitigates this risk by sharing 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.

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