United States Department of Justice (DOJ)

Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for
USA FOIAXpress

Issued by:

Kevin Krebs, Senior Component Official for Privacy

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

Date approved: [May 14, 2021]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Executive Office of the United States Attorneys (EOUSA) Freedom of Information Act and Privacy Act Unit and each of the United States Attorney's Offices (USAOs) nationwide are implementing USA FOIAXpress to track and fulfill requests submitted pursuant to the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act of 1974, 5 U.S.C. § 552a (FOIA and Privacy Act Requests). FOIA and Privacy Act requests are submitted by members of the public seeking access to nonpublic EOUSA and USAO records.

FOIAxpress allows EOUSA to log and track the processing of each FOIA or Privacy Act request, using data entered by DOJ staff or automatically generated by the system about the request, the requester, or the EOUSA staff assigned to process the request. The system records the status of the request, processing deadlines, and other key events or data. The system may store internal and external correspondence, such as exempt memoranda and directions to attorneys and EOUSA staff, correspondence to individuals responsible for conducting searches for potentially responsive records, requests for records sent to staff, and copies of communications with the requester. EOUSA also uses FOIAXpress to store and manage copies of the nonpublic DOJ records that have been gathered in response to requests. These records may contain personally identifiable information (PII) about the requester or other individuals mentioned or discussed in the records or DOJ personnel.

A PIA is required by Section 208 of the E-Government Act because FOIAXpress is a new information technology, procured by the Department, which involves the collection, maintenance, and dissemination of information in identifiable form.

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 is used to process access requests submitted to EOUSA for records under the Freedom of Information Act, found at 5 U.S.C. § 552, the federal access law that requires the full or partial disclosure of previously unreleased information and documents controlled by federal agencies, and the Privacy Act, found at 5 U.S.C. § 552a, the federal law that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

FOIAXpress is a commercial off-the-shelf, web-based application owned and operated by AINS Inc. AINS administers and maintains the application and all physical systems, and securely hosts EOUSA and USAO data. Select EOUSA staff and authorized individuals in the various USAOs access FOIAXpress through a secured website available only through the DOJ network. FOIAXpress is also built to include a Public Access Link (PAL), which will be integrated into FOIA.gov. This limited-use web portal permits members of the public access into the system to electronically submit their request, track its status and obtain correspondence sent from EOUSA staff. Requesters may create a PAL account with a unique login ID and

password so that they may submit requests for information electronically. Requesters may also attach supporting documentation to their request and directly download the documents through PAL if and when the documents are released by EOUSA.

The PAL portion of FOIAXpress is publicly accessible through the Internet; however, requesters do not have the ability to access any other data stored in FOIAXpress. Only authorized EOUSA FOIA and Privacy Act personnel have access to the data supplied by requesters via FOIAXpress. FOIA and Privacy Act requesters have access to responsive records in the system only after EOUSA staff make disclosure determinations. Before such disclosure, staff may share such documents with other government agencies, Congress, or the records' original submitters in order to determine whether the materials are confidential or otherwise exempt from mandatory FOIA or Privacy Act disclosure.

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 USC § 301 • 5 U.S.C. § 552 • 5 U.S.C. § 552a • 44 U.S.C. § 3301 (for the purposes of implementing provisions of 5 U.S.C. 552 and 5 U.S.C. 552a) • 28 U.S.C. § 35 • 44 U.S.C. § 21, 25, 27, 29, 31, and 33
	Executive Order	
	Federal Regulation	• 28 C.F.R. Part 16 • 28 C.F.R. Part 17
	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	A, B, C, and D	Full Names of DOJ users, federal employees referring requests, PAL requesters, and individuals mentioned in FOIA and Privacy Act records (responsive records) may be included.
Date of birth or age	X	A, B, C, and D	Date of birth or age of PAL requesters and individuals mentioned in responsive records may be included.
Place of birth	X	A, B, C, and D	Place of birth of PAL requesters and individuals mentioned in responsive records may be included.
Gender	X	A, B, C, and D	Gender of individuals mentioned in responsive records may be included.
Race, ethnicity or citizenship	X	A, B, C, and D	Race, ethnicity or citizenship of PAL requesters and individuals mentioned in responsive records may be included..
Religion	X	A, B, C, and D	Religion of individuals mentioned in responsive records may be included.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Social Security Number (full, last 4 digits or otherwise truncated) of requesters and individuals mentioned in responsive records may be included.
Tax Identification Number (TIN)	X	A, B, C, and D	Tax Identification Number (TIN) of requesters and individuals mentioned in responsive records may be included.
Driver's license	X	A, B, C, and D	Driver's license information of individuals mentioned in responsive records may be included.
Alien registration number	X	A, B, C, and D	Alien registration numbers of individuals mentioned in responsive records may be included.
Passport number	X	A, B, C, and D	Passport numbers of individuals mentioned in responsive records may be included.

(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 individuals mentioned in responsive records may be included.
Vehicle identifiers	X	C and D	VINs and license plate numbers mentioned in responsive records may be included.
Personal mailing address	X	A, B, C, and D	Personal mailing addresses of individuals mentioned in responsive records may be included.
Personal e-mail address	X	A, B, C, and D	Personal e-mail addresses of individuals mentioned in responsive records may be included.
Personal phone number	X	A, B, C, and D	Personal phone numbers of individuals mentioned in responsive records may be included.
Medical records number	X	A, B, C, and D	Medical records numbers of mentioned in responsive records may be included.
Medical notes or other medical or health information	X	A, B, C, and D	Medical notes or other medical or health information mentioned in responsive records may be included.
Financial account information	X	A, B, C, and D	Financial account information of individuals mentioned in responsive records may be included.
Applicant information	X	A, B, C, and D	Applicant information of individuals mentioned in responsive records may be included.
Education records	X	A, B, C, and D	Education records of individuals mentioned in responsive records may be included.
Military status or other information	X	A, B, C, and D	Military status or other information of individuals mentioned in responsive records may be included.
Employment status, history, or similar information	X	A, B, C, and D	Employment status, history, or similar information of individuals mentioned in responsive records may be included.

(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 performance ratings or other performance information, e.g., performance improvement plan	X	A and B	Performance improvement plan, warnings or reprimands of individuals mentioned in responsive records may be included.
Certificates	X	A, B, C, and D	Certificates mentioned in responsive records may be included.
Legal documents	X	A, B, C, and D	Legal documents mentioned in responsive records may be included.
Device identifiers, e.g., mobile devices	X	A, B, C, and D	Device identifiers mentioned in responsive records may be included.
Web uniform resource locator(s)	X	A, B, C, and D	Web uniform resource locator(s) mentioned in responsive records may be included.
Foreign activities	X	A, B, C, and D	Foreign activities of individuals mentioned in responsive records may be included.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Criminal records information of individuals mentioned in responsive records may be included.
Juvenile criminal records information	X	A, B, C, and D	Juvenile criminal records information of individuals mentioned in responsive records may be included.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	Civil law enforcement information mentioned in responsive records may be included.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, and D	Whistleblower information mentioned in responsive records may be included.
Grand jury information	X	A, B, C, and D	Grand jury information mentioned in responsive records may be included.
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 mentioned in responsive records may be included.
Procurement/contracting records	X	A, B, C, and D	Procurement/contracting records mentioned in responsive records may be included.

(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
Proprietary or business information	X	A, B, C, and D	Proprietary or business information mentioned in responsive records may be included.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	Location information mentioned in responsive records may be included.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Photographs or photographic identifiers of individuals mentioned in responsive records may be included.
- **Video containing biometric data**	X	A, B, C, and D	Video containing biometric data of individuals mentioned in responsive records may be included.
- **Fingerprints**	X	A, B, C, and D	Fingerprints of individuals mentioned in responsive records may be included.
- **Palm prints**	X	A, B, C, and D	Palm prints of individuals mentioned in responsive records may be included.
- **Iris image**	X	A, B, C, and D	Iris images of individuals mentioned in responsive records may be included.
- **Dental profile**	X	A, B, C, and D	Dental profiles of individuals mentioned in responsive records may be included.
- **Voice recording/signatures**	X	A, B, C, and D	Voice recordings/signatures of individuals mentioned in responsive records may be included.
- **Scars, marks, tattoos**	X	A, B, C, and D	Scars, marks, tattoos of individuals mentioned in responsive records may be included.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, and D	Vascular scans of individuals mentioned in responsive records may be included.
- **DNA profiles**	X	A, B, C, and D	DNA profiles of individuals mentioned in responsive records may be included.

(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 (specify)**	X	A, B, C, and D	Because of the varied nature of the records subject to disclosure, other types of PII not listed above may be collected, maintained or disseminated.
System admin/audit data:			
- **User ID**	X	A, B, C, and D	User ID of DOJ users and PAL requesters
- **User passwords/codes**	X	A, B, C, and D	User passwords/codes of DOJ users and PAL requesters
- **IP address**	X	A, B, C, and D	IP address of DOJ users, Federal Employees referring requests, and PAL requesters
- **Date/time of access**	X	A, B, C, and D	Date/time of access of DOJ users, Federal Employees referring requests and PAL requesters
- **Queries run**	X	A, B, C, and D	Queries run of DOJ users and PAL requesters
- **Content of files accessed/reviewed**	X	A, B, C, and D	Content of files accessed/reviewed of DOJ users and PAL requesters
- **Contents of files**	X	A, B, C, and D	Contents of files of DOJ users and PAL requesters
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Because of the varied nature of the records subject to disclosure, other types of PII not listed above may be collected, maintained or disseminated.

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	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): If an individual is represented by an attorney, the attorney may provide information on the client's behalf. Because the attorney acts as the client's representative, EOUSA considers any personal information provided by an attorney as submitted by the individual client.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Other federal entities that are consulting with or referring FOIA-requested records to EOUSA for processing.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): Any of the above categories may be FOIA requesters submitting requests that will be stored in FOIAXpress. Additionally, records that are responsive to FOIA requests, which are also stored in the system, may consist of information provided by the above sources.					

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		X	Information may be shared within the component during the routine processing of FOIA and Privacy Act requests. Responsive information may be shared within the component for review prior to disclosure.

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.**
DOJ Components	X			Responsive information that originated with other components may be transmitted by email for their review and approval or denial prior to disclosure.
Federal entities	X			Responsive information that originated with other agencies may be transmitted by email for their review and approval or denial prior to disclosure.
State, local, tribal gov't entities	X			Responsive information that originated with Tribal governments may be transmitted by email for their review and approval or denial prior to disclosure.
Public	X			Responsive information may be sent to members of the public through the PAL if they are the appropriate party for disclosure.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Responsive information may be sent to counsel or parties by secure email if they are the appropriate party for disclosure.
Private sector	X			Responsive information may be sent to corporate counsel or a corporation's agent by secure email if they are the appropriate party for disclosure.
Foreign governments	X			Responsive information may be sent to a foreign official by secure email if they are the appropriate party for disclosure.
Foreign entities	X			Responsive information may be sent to a foreign entity by secure email if they are the appropriate party for 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.

Not applicable.

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.

The information collection, use, and sharing activities as outlined in this PIA are covered by the following SORN:

DOJ-004: Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records. Last published in full at 77 FR 26580 (May 4, 2012). See: https://www.govinfo.gov/content/pkg/FR-2012-05-04/pdf/2012-10740.pdf.

Additionally, a Privacy Act § 552a(e)(3) notice is provided at the point-of-collection to members of the public entering information into the system.

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.

Individuals may decline to provide information, but a lack of necessary information may result in denial of the individual's FOIA or Privacy Act request until additional identifying information on the individual is provided.

Both the SORN and the Privacy Act § 552a(e)(3) notice, provided at the point-of-collection, informs the individual about their ability to decline to provide information and the consequences of doing so.

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 may request access to information in the system pertaining to them by visiting the following website for component-specific instruction: https://www.justice.gov/usao/resources/making-foia-request.

Additional information regarding access to information may be found in the following SORN:

DOJ-004: Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records. Last published in full at 77 FR 26580 (May 4, 2012). https://www.govinfo.gov/content/pkg/FR-2012-05-04/pdf/2012-10740.pdf.

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):** ATO: USA FOIAXpress; granted February 22, 2021; expires February 5, 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:** EOUSA has not initiated any POAMs for FOIAXpress as of the date of this document's publication.
	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:** FedRAMP moderate baseline controls have been implemented.
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:** FOIAxpress will audit and create logs for all activities within the system. The FOIAxpress Information System Security Officer (ISSO) will be responsible for reviewing all audit logs on a weekly basis.
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:** All internal users will complete general information security and privacy training, as well as training specific to the system.

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?

Access controls will be implemented to ensure that only authorized users have access to the information collected. Authorized users will only be granted the privileges necessary to accomplish their job duties. Individuals with access to FOIAXpress include external users, Attorney Advisors, Government Information Specialists, intake staff, FOIA Officers and administrators. Only administrators have privileged permissions to create, edit, and delete templates, fields, dashboards, and other various configurations within the application. Administrators also have the permission to create, edit, and delete users and user groups. Attorney Advisors, Government Information Specialists, and intake staff have the ability to create, edit and delete individual requests. The system is able to track access and create logs of user activity. In addition, there are other safeguards implemented, such as PIV access, in order to ensure that unauthorized access to the system is not granted and the risk of unauthorized disclosure of the information within the system is minimized.

Accounts will be locked after three unsuccessful login attempts to the system to ensure unauthorized users are prevented from forcing their way into the system by attempting multiple passwords. All login actions will be audited to ensure that no unauthorized users have been granted access to the system, and all audit logs are reviewed on a weekly basis by the ISSO. An open session within the information system will also be subject to session termination in cases of inactivity.

The PAL portion of FOIAXpress is publicly accessible through the Internet; however, requesters do not have the ability to directly access any other data stored in FOIAXpress. Only authorized EOUSA FOIA and Privacy Act Unit personnel have access to the data supplied by requesters via FOIAXpress.

Additionally, all sensitive information is automatically encrypted within FOIAXpress. The encryption itself is also tested, based on security controls, during the assessment process and prior to system authorization. Other security control families that are tested and implemented as safeguards include: Auditing, Contingency Planning, Incident Response, Media Protection, Physical Protection, Risk Assessment, and System and Information Integrity.

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.)

The data in FOIAxpress is maintained for as long as needed by the authorized USAO or EOUSA project requester and is subject to the respective retention periods that govern the relevant category of record, e.g., NARA General Records Schedules, agency Records Disposition Schedules (SF-115s), and any applicable SORNs published under the Privacy Act

of 1974, 5 U.S.C. §552a (see https://www.justice.gov/opcl/doj-systems-records). Procedures have been developed to ensure that electronic copies are not, in practice, retained beyond the retention period established for the original records and will be disposed of in accordance with DOJ Network Account Records Management USAP No. 3-13.300.004.

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:

DOJ-004: Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records. Last published in full at 77 FR 26580 (May 4, 2012). See: https://www.govinfo.gov/content/pkg/FR-2012-05-04/pdf/2012-10740.pdf.

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.***

The collection, maintenance, disclosure, and sharing of information in FOIAXpress inherently increases risks to privacy, such as unauthorized modification, disclosure, and breach of personal information. However, EOUSA takes measures designed to reduce those privacy risks.

All EOUSA component systems, including FOIAXpress, are subject to consistent assessment and authorization processes that ensure that security controls are in place to protect the confidentiality, integrity, and availability of all information and the systems that house that information. For

example, access controls based on the principle of least privilege will be implemented to ensure that only authorized users have access to the information collected and to ensure that those who have access to the system are only granted the minimum access required based on job duties.

FOIAXpress users are provided regular trainings by the Justice Management Division on appropriate disclosures and all EOUSA component staff are required to complete mandatory security awareness, privacy, and role-based training on an annual basis. Additionally, all sensitive information is automatically encrypted within FOIAXpress. The encryption itself is also tested, based on security controls, during the assessment process and prior to system authorization. Other security control families that are tested and implemented as safeguards include: Auditing, Contingency Planning, Incident Response, Media Protection, Physical Protection, Risk Assessment, and System and Information Integrity.

The FOIA and Privacy Act Unit includes contractors who can create, collect, use, process, store, maintain, disseminate, disclose, and dispose of information within FOIAXpress under the direction of Federal employees. To mitigate the risk of unauthorized modification or disclosure of DOJ data, contractors will not have access to the system unless it is necessary for the administration and processing of access requests, or to ensure the proper functioning of the system. In that case, specific access will be granted and removed when the necessary work has been completed. All DOJ contractors are required to abide by standard clauses regarding the protection of individual privacy from the Federal Acquisition Regulation (FAR). Additionally, all contractors are provided annual privacy and security training.

Authorized AINS staff have access to servers containing DOJ data to perform maintenance and troubleshooting activities. To mitigate the risk of unauthorized disclosure, these staff have signed non-disclosure agreements with DOJ. Based on information provided by AINS, EOUSA understands that AINS staff are also required to take AINS's annual security training. Specific DOJ data that is maintained within FOIAXpress is encrypted and not generally accessible to AINS staff. However, in the event of a system issue, AINS staff may be granted access to view DOJ data in order to fix specific issues.

In order to minimize the risk of unauthorized disclosures to the public, FOIA and Privacy Act requesters are provided access to responsive records in FOIAXpress only after EOUSA staff make the appropriate disclosure determinations. Prior to such determination, staff may share responsive records with other government agencies, Congress, or the records' original submitters in order to determine whether the materials are confidential or otherwise exempt from mandatory FOIA or Privacy Act disclosure.