United States Department of Justice (DOJ)

Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for the
USAfx File Exchange (USAfx)

Issued by:
Senior Component Official for Privacy - Kevin S. Krebs

Approved by: Christina Baptista, Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: December 6, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The USA File Exchange ("USAfx") permits authorized users to exchange electronically stored information ("ESI") with outside entities more efficiently and quickly than previously possible through a secure web-based portal that automatically encrypts data both in transit and at rest. The Box Enterprise Cloud Content Collaboration Platform ("Box") is the core component of the USAfx system. USAfx is a file exchange system – not a file storage system – intended solely for the short-term transfer of sensitive ESI for official business purposes. All documents intended for file exchange are subject to the USAfx short-term retention policy which is applied at a system level within the USAfx application. After the retention period passes, all file exchange documents are removed from the system.

USAfx is a Software as a Service (SaaS) cloud solution that is hosted and managed by Box, Inc. The infrastructure or Platform as a Service (PaaS) hosting USAfx is also owned by Box. USAfx will be used to exchange mission or case-related data between internal and external users in a controlled and secure manner.

Given the multitude of data elements that may be exchanged in the course of a case, USAfx could foreseeably implicate almost any type of PII, as described in the table in Section 3.1.

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.

USAfx will be used to exchange mission or case-related data between internal and external users in a controlled and secure manner. USAfx is a secure file exchange system – not file storage – intended solely for the short-term transfer of sensitive ESI for official business purposes. The primary use case of the USAfx system is to facilitate the exchange of case materials, including the delivery of eDiscovery documents, but the system may also be used internally to exchange documents and files through an easy-to-use platform. All documents intended for file exchange are subject to the USAfx short-term retention policy which is applied at a system level within the USAfx application. After the retention period passes, all file exchange documents are automatically removed from the system. Users can extend the retention period for files, but not for folders. By default, files can be set to extend by 7 days, 1 month, or 1 year. Users can also choose a custom expiration date with no limit. Indefinite retention of folders is governed by a policy rule and is restricted to USAfx Program Management folders or designated folders approved by the USAfx Program Manager.

To facilitate easier compliance with DOJ policy, and in support of data encryption requirements, the system transmits and stores all data in an encrypted state.

The general categories of information that may be personally identifiable that could be contained within USAfx include but are not limited to contact information, personal identifiers,

and basic biographical information. These categories of information that may be contained within USAfx are potentially related to DOJ/Component Employees, Contractors, and Detailees, Other Federal Government Personnel, Members of the Public - US Citizens or Lawful Permanent Residents (USPERs), and/or Members of the Public - Non-USPERs, and would generally be uploaded as part of case files or pre-employment security packages.

Additionally, as the primary use case of USAfx is to exchange case-related documents, the nature of personal information that may be contained within the contents of these documents varies greatly. This can include but is not limited to such sensitive information as name, address, previous addresses, driver's license and/or passport numbers, sex, religion, SSN/TIN, financial records and statements, medical records, and education records. The sources of this sensitive information also vary greatly and may be provided directly to government sources by the individual through the legal process (e.g. discovery) or by submitting applications and forms to government agencies. Information may also have been subpoenaed from third-party sources.

As previously stated, the primary use case of the USAfx system is to facilitate the exchange of case materials, including the delivery of eDiscovery documents, but the system may also be used internally to exchange documents and files through an easy-to-use system. Pre-employment security packages may be uploaded and accessed by Internal users only, to facilitate providing these documents securely to personnel security & HR teams. Case files are accessed by both Internal Users and External Users that fall under categories of External Adverse, External Trusted, and Grand Jury. These groups are made up of non-federal counsel representing opposition to the government, users working with the federal government, and Grand Jury reporters.

USAO users have the ability to sponsor external public-facing users for accounts within USAfx. To sponsor the external user, the USAO user will collect their name, e-mail address, and input this information into the system to create the sponsored account.

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	• 5 USC § 301 • 44 USC § 3301 (for the purposes of implementing provisions of 5 U.S.C. 552 and 5 U.S.C. 552a) • 28 USC Ch. 35 • Federal Information Security Modernization Act of 2014, 44 USC § 101 note
Executive Order	Homeland Security Presidential Directive 12
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	

Other (summarize and provide copy of relevant portion)	• DOJ Order 0903: Information Technology Management • DOJ Order 0904: Cybersecurity Program

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	This category of information may be included in files/data uploaded to the system. Names are collected for the creation/maintenance of user accounts within the system.
Date of birth or age	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Place of birth	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Sex	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Race, ethnicity, or citizenship	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Religion	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Tax Identification Number (TIN)	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.

(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
Driver's license	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Alien registration number	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Passport number	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Mother's maiden name	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Vehicle identifiers	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Personal mailing address	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Personal e-mail address	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Personal phone number	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Medical records number	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Medical notes or other medical or health information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Financial account information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Applicant information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Education records	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Military status or other information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Employment status, history, or similar information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.

(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
Certificates	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Legal documents	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Device identifiers, e.g., mobile devices	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Web uniform resource locator(s)	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Foreign activities	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Juvenile criminal records information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Grand jury information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Procurement/contracting records	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Proprietary or business information	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
Biometric data:	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Photographs or photographic identifiers**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.

(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
- **Video containing biometric data**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Fingerprints**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Palm prints**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Iris image**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Dental profile**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Voice recording/signatures**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Scars, marks, tattoos**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **DNA profiles**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **Other (specify)**	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
System admin/audit data:	X	A, B, C, and D	This category of information may be included in files/data uploaded to the system.
- **User ID**	X	A, B, C, and D	User ID of internal and external users.
- **User passwords/codes**	X	A, B, C, and D	User passwords/codes of internal and external users.
- **IP address**	X	A, B, C, and D	IP addresses of internal and external users.
- **Date/time of access**	X	A, B, C, and D	Date/time of access of internal and external users.
- **Queries run**	X	A	Queries run by internal users (administrators)
- **Contents of files**	X	A, B, C, and D	Contents of files of internal and external users.
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		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify): information is collected directly from users to establish accounts in USAfx					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

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

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			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).

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			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).

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.**
Federal entities	X			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).

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.**
State, local, tribal gov't entities	X			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).

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.**
Public	X			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).

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			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).

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.**
Private sector	X			When a user is granted an account in USAfx, they are given access to share files with other users of the system. A user account is required to access any data within the system. To login to the system, every user is forced to enter a username, password, and MFA, or a PIV certificate-based secure logon method. Once the user is authenticated into the system, they may create folders and share these folders with others, or they may have folders shared with them. Users create their own folders, and control sharing rights inside of folders for each individual invited into a folder. Users with upload permissions within a folder are the only users who may add contents to that folder. Every file that is uploaded within to USAfx is encrypted both in transit, and at rest. Only those users that have had a file or folder shared with them will have access – the user who owns the folder can customize who has access and at what level(s).
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.

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.

There are two distinct classes of information that may be in the USAfx system. While USAfx does not collect the data in either case, the data nevertheless resides in the USAfx system.

The first class of information is user account information; the names and e-mail addresses of all users in the system is collected via the USAidgov-gc (USA Identity Governance - GC) and USAauth applications.

The second class of information is data that is uploaded by users into the USAfx system, and stored in the systems cloud storage. This data is mission or case-related files and uploads, and may or may not be directly collected from individuals, as the source of mission or case-related files and uploads is not governed by USAfx itself.

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.

The use of USAfx is voluntary. Individuals are not required to participate in the use of the system. The names and e-mail addresses of all users of the system is collected via the USAidgov-gc (USA Identity Governance - GC) and USAauth applications. I If a user does not want to utilize USAfx, they can opt not to provide their name and e-mail address information and subsequently would not receive an account within USAfx. The system is generally used as a secure way to share and exchange information with authorized recipients. While individuals may have opportunities to consent to the collection of the information or specific uses, individuals do not necessarily have opportunities to limit the use of this system as a mechanism to share the information.

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.

Users may contact their account sponsor to have their name or e-mail address information

corrected within USAfx.

Access to the information is permitted only through 5 USC 552 (Freedom of Information Act "FOIA") and controlled by staff of EOUSA's Freedom of Information/Privacy Act Office. The information must be requested through a formal process documented at https://www.justice.gov/usao/resources/making-foia-request. This process ensures administrative and physical controls.

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 source 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 last ATO was completed April 2, 2024 and will expire on April 2, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **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:** Not Applicable.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** USAfx has an overall FISMA security categorization of moderate based on the types of information it contains (Litigation and Judicial Activities), and consequently, EOUSA has implemented FedRAMP moderate baseline controls for the system. The implemented controls undergo control assessments on an annual basis to ensure they are properly implemented. Assessment includes vulnerability testing, compliance monitoring, and control evaluation.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** FedRAMP Moderate baseline controls are implemented. Implementation of controls is documented in the USAfx System Security Plan and controls are assessed to ensure these controls are operating as intended. Core controls (subset of controls identified by the agency) are assessed annually. All controls (including core

	controls) are assessed every three years before re-authorization of the system is presented for approval to the Authorizing Official.
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:** USAfx audits and create logs for all activities within USAfx. The USAfx Information System Security Officer (ISSO) is responsible for reviewing all audit logs on a weekly basis. Activities include but are not limited to: Login, Failed Login, Rejected Terms of Service, Add Login app, login verification enabled/disabled, file copied, file moved to trash, file downloaded, file edited, file locked, file moved, file previewed, file renamed, file uploaded, etc.
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:** General information security and privacy training and training specific to the system for authorized users within the Department. There are USAfx training guides and job aids for end users, account requests (for all account types), expert witnesses, external DOJ users, jury reporters, etc.

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 are implemented to ensure only authorized users have access to the information collected, in addition to only being granted the privileges necessary to accomplish their job duties. These controls include but are not limited to account management, account approval, least privilege, Additionally, there are safeguards, described below, that are implemented 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.

USAfx is integrated with USAauth (Okta) and users utilize MFA (multifactor authentication) to access the application. All login actions are 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 system ISSO. An open session within the USAfx system will also be terminated after periods of inactivity.

Audit logs contain details regarding user logins, rejecting or accepting terms of service, downloading login app, login failure, uploads, downloads, file copied, deletions, file re-name, privileged actions (if applicable). Privileged actions include policy changes, user deletions, file

and folder deletions, among others.

Details included in logs are date, user name, user email, affected, affected ID, size, , IP address, parent folder, action, and details.

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 the USAfx system is maintained for as long as needed by the authorized DOJ users and are subject to the respective retention periods that govern them, e.g., NARA General Records Schedules, agency 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 USAPP No. 3-13.300.004

Users are kept on file for 90 days after their last activity. After 90 days of inactivity, their USAfx account is disabled. If they do not request access within 30 days of their account being disabled, their account is permanently deleted. Audit logs are retained for up to 7 years. and metadata, work with JB on this. Users can extend the retention period for files, but not for folders. Files are subject to a retention policy of 60 days. By default, files can be set to extend by 7 days, 1 month, or 1 year. Users can also choose a custom expiration date with no limit. Indefinite retention of folders is governed by a policy rule and is restricted to USAfx Program Management folders or designated folders approved by the USAfx Program Manager.

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).

__X___ No. _____ 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-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009), available at https://www.gpo.gov/fdsys/pkg/FR-2009-11-04/pdf/E9-26526.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?

The disclosure or sharing of information increases risks to privacy. However, there are measures taken to reduce the risk of unauthorized disclosure and potential data breach. All EOUSA component systems 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. The USAfx audit logs are reviewed on a weekly basis for any anomalous and/or suspicious activity.

Access controls are in place for all file access. Users can not view or edit folders and files without the appropriate permissions assigned for specific folders and files. These permissions are granted only by owners of the folders and files that have created them or have explicitly granted access to users for viewing or editing. This process ensures least privilege is enforced as users only have access to files to folders to which the user is allowed.

The principle of least privilege will be enforced to ensure those who have access are only granted the minimum access required based on job duties. All EOUSA component staff require mandatory security awareness and role-based training on an annual basis. Cybersecurity Awareness Training (CSAT) educates internal users on federal information privacy laws and requirements, such as the Privacy Act and requirements for prior handling of PII. Rules of Behavior are also required to be acknowledged by all internal users before being granted access to EOUSA systems. For all users, a warning banner is provided before being able to access USAfx.

Additionally, security controls will be tested 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.