Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Justice Enterprise File Sharing System

Issued by:
Arthur E. Gary
JMD General Counsel and Senior Component Official for Privacy

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [November 30, 2017]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The Justice Enterprise Files Sharing (JEFS) system uses the Box Incorporated ("Box")[1] Software as a Service (SaaS) capability[2] as a transport infrastructure for users to share securely most types of files within Department of Justice (DOJ or the Department) Components, between DOJ Components, and with external entities who have authority to access information maintained by the Department. The JEFS system can function across multiple platforms including smartphones, tablets, and workstations, anywhere inside or outside the DOJ network. The Department utilizes JEFS as a transport infrastructure only, and the Department has not designated the JEFS system as an official record-keeping system, a document archival system, or a document backup system.

The Department conducted this Privacy Impact Assessment (PIA) because the personally identifiable information (PII) collected, used, and maintained includes names, email addresses, and audit log information of DOJ employees and contractors, as well as names, email addresses, mobile phone numbers, and audit log information of non-DOJ end-users. Additionally, documents transferred through JEFS may include significant quantities of personal information relating to the substantive work of the Department. Because of the varied nature of the Department's work, documents transferred through JEFS could conceivably include almost any type of unclassified PII information. This PIA covers all Department Components' instances of JEFS.

Section 1: Description of the Information System

(a) The purpose that the records and/or system are designed to serve;

DOJ implemented JEFS to simplify secure internal and external file sharing with key stakeholders and third party organizations, (e.g., expert witnesses, co-counsel, and local law enforcement officers), and to support mobile and offline access to files regardless of location or device. The Department utilizes JEFS as a transport infrastructure only, and the Department has not designated JEFS as an official record-keeping system, a document archival system, or a document backup system.

(b) The way the system operates to achieve the purpose(s);

JEFS is a specially configured implementation of Box's SaaS capability that underwent a

---

[1] Box Inc. provides an enterprise content management platform that allows users to share and access files, while establishing specific data governance and retention policies for specific clients, such as DOJ. More information on Box can be found at: https://www.box.com/home.

[2] "SaaS" capabilities provide consumers with a provider's applications running on a cloud infrastructure. National Institute for Standards and Technology (NIST), Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. "The applications are accessible from various client devices through either a thin client interface, such as a web browser . . . or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings." *Id.*

rigorous security assessment and meets DOJ security requirements. JEFS enables users to upload up to 15 gigabytes of most file types—documents, videos, photos, etc.—from a phone, tablet or computer. Users can then access those files for up to 60 days[3] from anywhere through the DOJ network or over the Internet.

Box manages the hardware and software cloud environment, [4] and DOJ manages the front-end application of each instance of JEFS.

Each individual DOJ Component (e.g., the Federal Bureau of Investigation, the Bureau for Alcohol, Tobacco, Firearms, and Explosives, the Drug Enforcement Administration) manages its own JEFS instance, and purchases its own licenses directly from the vendor using a DOJ Blanket Purchase Agreement (BPA). Each Component also manages its own service desk and account administration. Accounts for users from DOJ Components that do not have their own JEFS instance are created under the Justice Management Division (JMD) JEFS instance. This PIA covers all the Department's JEFS instances.

(c) The type of information collected, maintained, used, or disseminated by the system;

The JEFS system collects, maintains, and uses the following information for DOJ users: user name and DOJ email address. The JEFS system collects, maintains, and uses the following information for non-DOJ users: user name, email address, and mobile phone number.

As detailed below in Section 6, the JEFS system also maintains audit logs of JEFS user activity such as logins, uploads, downloads, file rename, Internet Protocol (IP) address, and browser.

The particular data that passes through JEFS is Sensitive-But-Unclassified (SBU) at its highest classification. JEFS is not authorized to process, store, or transmit classified data. JEFS has a Security Categorization of Moderate based on the Federal Information Processing Standard Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.[5]

Because of the varied nature of the Department's work, the files shared via the JEFS system could conceivably include any type of SBU Moderate information; it is therefore not possible to list with certainty every item of information that users could potentially share via the system.

---

[3] Under limited, case-by-case circumstances, the JEFS System Owner, in consultation with the DOJ Office of the Chief Information Officer, Cybersecurity Services Staff, may grant a waiver to extend the 60-day retention period.

[4] "Cloud computing" is defined by NIST as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." *Id.* A "cloud environment" or "cloud infrastructure" is the "collection of hardware and software that enables the five essential characteristics of cloud computing." *Id.*

[5] A Security Categorization of Moderate means "the loss of confidentiality, integrity, or availability to this system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." *See* NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

However, JEFS will only handle information that the DOJ has the authority to share. The Department may share information within DOJ Components, between DOJ Components, and with external entities who have authority to access information maintained by the Department to accomplish an authorized function.

The JEFS system collects metadata about shared files, such as the file create date, but not the content of the files shared. Authorized files accessed for transport in and out of the JEFS system are deleted after 60 days through automated means.[6]

(d) Who has access to information in the system;

Access to JEFS is restricted to DOJ employees and contractors, and approved users from external entities outside DOJ. A user is granted a JEFS account only when approved by the DOJ Component Authorizing Official or designee. Additionally, some DOJ Components impose further requirements that must be met prior to granting a JEFS account. Only the DOJ JEFS Administrators have access to the information collected by the system as described in section 1.c.

(e) How information in the system is retrieved by the user;

Information in the JEFS system can be accessed using multiple platforms including smartphones, tablets, and desktop computers. Once authenticated into the JEFS system, JEFS users have access to files to which they have been granted explicit authorization (e.g., read only, edit, lock, password protect.) DOJ JEFS Administrators can retrieve audit log information by a JEFS user's name or email address. Once a user is successfully authenticated and logs into JEFS, the user sees the JEFS interface. A user can then use one of two methods to upload files and folders into JEFS: either a "drag and drop" method, or through a search for files through the user's file browser. To access a file already in JEFS, the user clicks on the desired folder or file.

(f) How information is transmitted to and from the system;

Every file is encrypted in transit between the user (independent of platform) and Box data centers with high-grade Secure Sockets Layer (SSL) encryption, compliant with the FIPS Publication 140-2.[7] Once encrypted data reaches the Box network, files are encrypted when stored ("at rest") at all times using the 256-bit Advanced Encryption Standard (AES).[8] All physical co-location facilities used as the primary processing facilities are located within the United States.

---

[6] *See supra* note 3.
[7] NIST FIPS 140-2 can be found at: http://csrc.nist.gov/groups/STM/cmvp/standards.html.
[8] AES "specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data." NIST FIPS 197, *Advanced Encryption Standard (AES)* (Nov. 2001), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. Specifically, the AES algorithm "is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext." *Id.*

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects);

The JEFS system interfaces with the DOJ's Active Directory Federation Services for the authentication of DOJ JEFS users when accessing the JEFS system from within the DOJ network.

(h) Whether it is a general support system, major application, or other type of system;

The JEFS system is categorized as a Major Application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Specific to JEFS user accounts, the JEFS system collects and maintains the following information:

- For DOJ JEFS users: User name, DOJ email address, IP address and browser
- For non-DOJ JEFS users: User name, email address, mobile phone number, IP address and browser. The mobile phone number is required because non-DOJ must go through a second factor authorization through Short Message Service texts when logging in from an unknown device.
- JEFS also maintains audit logs of user activity such as logins, uploads, and downloads.

Additionally, documents transferred through JEFS may include significant quantities of personal information relating to substantive work of the Department. Because of the varied nature of the Department's work, the JEFS system could be used to share any SBU Moderate information that a DOJ user has authorization to disclose to a recipient user. Consequently, it is not possible to list with certainty every item of information that will be disseminated by the system. Therefore, the items of the information checked below are limited to end-user account information and audit log information maintained by the JEFS system. Specific to the files shared via JEFS, the JEFS system collects metadata about files, such as the file create date, but not on the content of the files.

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			

Identifying numbers
Other identifying numbers (specify):

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number	X	Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number	X	Salary	
Job title		Email address	X	Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID		Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	
Other system/audit data (specify):	Browser type and modifications to JEFS system settings.				

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

The sources of the information in the JEFS system come from two distinct JEFS users: DOJ users and non-DOJ users. DOJ users include both DOJ employees and DOJ contractors. DOJ users are required to provide their name and a DOJ email address to obtain a JEFS account.

Non-DOJ users include employees of other federal agencies, employees of state or local government agencies, employees of a private company or law firm, or other external entities that have authorization to access particular information shared by DOJ users or authorization to transfer information to DOJ users. Non-DOJ users provide name, email address and mobile phone to obtain a JEFS account.

JEFS users upload files into JEFS as part of their substantive work for the Department. Though such files may come from any source(s), the JEFS system retains beyond the 60-day retention period only metadata about shared files,[9] such as the file create date, but not the content of the files shared. In JEFS, every file is encrypted in transit (a process that starts when the user clicks on the file to be uploaded, until it reaches the cloud service provider data centers) with high-grade SSL encryption, compliant with FIPS 140-2. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. The cloud service provider personnel can see the encrypted files and metadata about those files, such as the file create date, but not the information within the files themselves.

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

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy.

A potential threat to privacy in light of the information collected is that the system will collect

[9] *See supra* note 3.

and/or maintain more information than is relevant and necessary to accomplish the Department's official duties. JEFS is a transport infrastructure that does not exercise control over the contents of information shared; however, there are existing technical, administrative, and physical limits on the type of information that may be collected, including but not limited to, the statutory protections afforded certain information under the Privacy Act of 1974, as amended ("Privacy Act"), and DOJ policies.

JEFS is not designated as an official record-keeping system, a document archival system, or a document backup system. As such, authorized files accessed for transport in and out of the JEFS system are deleted in 60 days through automated means.[10] On a case-by-case basis, depending on the DOJ Component operating procedures, the deleted files may be restored by the DOJ Component JEFS Administrator up to 7 days after the automated deletion.

To prevent unauthorized access to JEFS, DOJ staff (employees and contractors) and approved users from external entities outside DOJ can have access to the JEFS system if approved by the DOJ Component Authorizing Official or designee, as detailed in Section 6. Additionally, some DOJ Components impose further requirements that must be met prior to granting a JEFS account.

To further mitigate potential risks associated with collecting or maintaining more information than is necessary to accomplish the Department's official duties, all JEFS inactive accounts are deleted after 90 days of inactivity.

Additionally, because JEFS users use the system to help carry out the Department's various missions, the type of files transported through the system are governed by the various authorities delineating component missions and authorizing the collection and maintenance of information to carry out such missions. These authorities are listed in the various Privacy Act system of records notices (SORN) that apply to the records maintained in a system of records transported via JEFS, depending on the nature of such files and how the information on the files is retrieved.

For information about the security controls that the Department applied to JEFS that assist in mitigating threats related to the collection of PII, please see the responses to questions 6.1 and 6.2, below.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

The JEFS system is only used as a transport infrastructure. It offers high volume short-term capabilities to share documents and most types of files among individuals within DOJ

[10] *See supra* note 3.

Components, between DOJ Components, and with external entities who have authority to access particular information shared by the Department. DOJ personnel use the JEFS system file sharing functionality in furtherance of the various missions of DOJ components. The JEFS system is not designated as an official record-keeping system, a document archival system, or a document backup system.

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	X	For administering human resources programs
X	For litigation		
X	Other (specify): To assist in the secure sharing of SBU Moderate files by DOJ Components to entities that have appropriate authorization to access such information in support of DOJ Component activity.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The breadth of the DOJ mission and the DOJ Components, including civil and criminal law enforcement, requires secure, timely, and effective communications and information sharing in support of the areas checked in question 3.1. DOJ personnel use the JEFS system file sharing functionality in furtherance of the various missions of DOJ components. Examples may include:

- to send and receive information from external entities including other US government agencies and other law enforcement organizations;
- to perform instant DOJ staff-to-staff transfer of law enforcement data that is typically too large to email;
- to share information with external entities including expert witnesses, opposing counsel, etc.;
- to exchange information with courts;
- to share information with external entities including vendors, consultants, attorneys, etc.;
- to transfer information to mobile devices or DOJ laptops for access to information in locations such as courts, senior leadership briefings, etc.;
- to receive job applicant materials;
- to deliver information to DOJ staff in other components;
- to exchange IT-related files such as source code, log files, etc.; and
- to disseminate training materials.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	5 U.S.C. § 301; 44 U.S.C. § 3101
	Executive Order	
	Federal Regulation	
X	Memorandum of Understanding/agreement	Justice Enterprise File Sharing Memorandum of Agreement between DOJ and Components.
X	Other (summarize and provide copy of relevant portion)	Various DOJ component mission authorities (including statutes, Executive Orders, and regulations). DOJ Order 0904 – Cybersecurity Program; DOJ Order 2740.1A – Use and Monitoring of DOJ Computers and Computer Systems; DOJ Order 0903 Information Technology Management; DOJ Order 2880.1C – Information Resources Management Program 1 C Chapter 2, section 16.

3.4 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 JEFS system is not designated as an official record-keeping system, a document archival system, or a document backup system. As such, authorized files accessed for transport in and out of the JEFS system are deleted in 60 days through automated means.[11]

Box Inc. stores audit logs of system administration/audit information (including user account information) for a period of 7 years or until the front-end application/system is removed. In accordance with the DOJ IT Security Standards, JEFS audit logs of administration/audit information (including user account information) sent to DOJ are retained for a minimum of 1 year online and 30 days offline (in backup storage). The Department would ingest logs into the

[11] *See supra* note 3.

DOJ Justice Management Division, Cybersecurity Services Staff Splunk instance.[12]

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The JEFS system provides users with the ability to share files over the web, via a standard web-browser, and through a mobile interface such as a native mobile application (available on iOS, Android, Windows mobile OS, and Blackberry devices). Potential threats to privacy when sharing files via the JEFS system include unauthorized disclosure of information.

To ensure authorized use of JEFS, DOJ staff and approved users from external entities outside DOJ can have access to the JEFS system if approved by the DOJ Component Authorizing Official or designee. Additionally, some Components may impose further requirements prior to granting a JEFS account.

To ensure that the information is handled, retained, and disposed of appropriately, users take mandatory computer training annually which includes training on the Privacy Act and the Cybersecurity Executive Branch Order. Additionally, JEFS users agree at least annually to the JEFS Terms of Usage that include General Rules of Behavior and a link to the Department of Justice Website Privacy Policy.[13]

To protect files shared via JEFS, the system has built controls that ensure every user can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a particular file. Every time a user attempts to access a file or folder (by clicking on the file on the JEFS interface which is displayed after the user has successfully authenticated into the system), JEFS uses these permissions to verify that a user has explicit authorization to interact with the file and what specific interaction permissions (e.g., read-only). This process ensures that a user has access only to the files or folders to which the user is allowed and that the user is restricted to the authorized type of interaction with the specific files or folders.

In JEFS, every file is encrypted in transit (the process that starts when the user clicks on the file to be uploaded, until it reaches the cloud service provider data centers) with high-grade SSL encryption, compliant with FIPS 140-2. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. All physical co-location facilities used as the primary

[12] The Department's Splunk instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.
[13] The DOJ Website Privacy Policy can be found here: https://www.justice.gov/doj/privacy-policy.

processing facilities are located within the United States. The cloud service provider personnel can see the encrypted files and metadata about those files, such as the file create date, but not the information within the files themselves.

JEFS audit logs are available on a read-only mode to designated DOJ JEFS privileged users. DOJ JEFS privileged users such as JEFS Administrators and JEFS Information System Security Officers review JEFS audit logs for security monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate system activity. JEFS audit logs are automatically monitored by Box's Security Incident and Event Management (SIEM) tool. Any alteration of JEFS audit logs would be flagged by the SIEM.

Authorized files accessed for transport in and out of the JEFS system are deleted after 60 days through automated means.[14] In addition, each DOJ Component with a JEFS instance can further customize the security and permissions of its files. For example, DOJ Components with a JEFS instance can specify when a user can only upload files into a folder without the ability to view other files on the folder; specify that a file can only be shared only with users with a usdoj.gov domain email address; or prohibit downloads of a certain file. Overall, JEFS users are given only the privileges they need to access a file and the file is deleted through automated means.

Additionally, the JEFS system has automated functionality to place files that may contain Social Security Numbers (SSNs) or files with words/phrasing similar to security markings higher than SBU (e.g., Top Secret) into a restricted "Quarantine" area. The files will then require action from a JEFS Administrator before they become available for use.

For a list and description of security controls that have been put into place to safeguard against these and other risks (including mandatory training for system users regarding appropriate handling of information and automatic purging of information), please see the responses to questions 6.1 and 6.2.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			
Federal entities	X			

[14] *See supra* note 3.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
State, local, tribal gov't entities	X			
Public	X			
Private sector				
Foreign governments				
Foreign entities	X			Foreign nationals may obtain a JEFS account with approval from both the Department of Justice Chief Information Officer (CIO) and the Department of Justice Security Officer (DSO).
Other (specify):	X			Any other external entity that is authorized to establish a JEFS account and has the authority to receive information maintained by DOJ, such as outside experts or parties in litigation.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

To prevent or mitigate threats to privacy in connection with the disclosure of information, each DOJ Component that operates a JEFS instance signs a JEFS Memorandum of Agreement (MOA) with JMD. In the JEFS MOA, the DOJ Component agrees to comply with the requirements of the JEFS Authority to Operate (ATO). The DOJ Component further certifies that its own policies, if any, governing end users' access to, or appropriate use, handling, dissemination, and/or destruction of information pertaining to JEFS align with DOJ system requirements.

In addition, each user must also agree at least annually to the DOJ Terms of Usage that include the DOJ General Rules of Behavior and a link to the Department of Justice Website Privacy Policy. Additionally, every page in JEFS, including the JEFS login page, displays a link to the Department of Justice Website Privacy Policy.

By Department Order, all DOJ users working on Department systems including JEFS, must receive an annual Computer Security Awareness Training (CSAT) course. The CSAT course includes information on certain federal information privacy laws and requirements, such as the Privacy Act and requirements for proper handling of PII.

JEFS has built controls that ensure every user can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, JEFS uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed; and that the user is restricted to the authorized type of interaction (e.g. read-only) with the specific files or folders.

To prevent or mitigate threats to privacy in connection with the disclosure of information, the JEFS system has automated functionality to place files that may contain SSNs or files with words/phrasing similar to security markings higher than SBU (e.g. Top Secret) into a restricted "Quarantine" area. These files will then require action from a JEFS Administrator before they become available for use. Additionally, responses to potential unauthorized disclosures or data breaches are covered in vendor contracts.

JMD maintains the security certification and accreditation of the system. For a list and description of security controls that have been put in place in order to prevent or mitigate threats to privacy in connection with the disclosure of information, as well as to safeguard against other threats to privacy, please see the responses to questions 6.1 and 6.2.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: A warning banner notifies JEFS end-users at login that any information transmitted through the system may be monitored, intercepted, searched, and/or seized by the Department and that users therefore have no reasonable expectation of privacy in such information. Additionally, once a year, JEFS users must consent to the JEFS Terms of Use and the DOJ Rules of Behavior. Specific to files shared via JEFS, the JEFS system is only used as a transport infrastructure with no processing and it is not designated as an official record-keeping system,

		a document archival system, or a document backup system. As such, the notification to individuals is governed by the various authorities delineating DOJ Component missions and authorizing the collection and maintenance of information to carry out such missions.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Specific to information collected by JEFS, such as the user name and email address, DOJ personnel may choose to use a means to share files other than the JEFS system (e.g. email, phone, fax, other systems, etc.). Moreover, non-DOJ individuals may choose not to use the JEFS system to share files with DOJ users. Specific to files shared via JEFS, the JEFS system is only used as a transport infrastructure with no processing and it is not designated as an official record-keeping system, a document archival system, or a document backup system. As such, the opportunity to decline to provide information contained in the files shared via JEFS is governed by the various authorities delineating DOJ Component missions and authorizing the collection and maintenance of information to carry out such missions.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: JEFS users provide consent when they agree to the JEFS Terms of Usage and the DOJ Rules of Behavior. Specific to files shared via JEFS, the JEFS system is only used as a transport infrastructure with no processing and it is not designated as an official record-keeping system, a document archival system, or a document backup

		system. As such, the opportunity to decline to consent to particular uses of the information contained in the files shared via JEFS is governed by the various authorities delineating DOJ Component missions and authorizing the collection and maintenance of information to carry out such missions.
	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

To provide transparency and allow JEFS users to understand how their communications and other information are handled, the following is in place:

- The DOJ security-warning banner is displayed on the login screen that JEFS users see when they log into the JEFS system. The DOJ warning banner informs users that any information that they transmit through a computer or mobile device, including information transmitted through JEFS, may be monitored, intercepted, searched, and/or seized by the Department, and that JEFS users therefore have no reasonable expectation of privacy while using the system.

- Additionally, the JEFS Terms of Usage is also displayed when a user first logs in and at a minimum annually thereafter. The JEFS Terms of Usage inform users that any information that they transmit through a computer or mobile device, including information transmitted through JEFS, may be monitored, intercepted, searched, and/or seized by the Department, and that JEFS users therefore have no reasonable expectation of privacy in such communications.

- The JEFS Account Request Form template includes the DOJ Rules of Behavior (ROB) that users sign prior to submitting the account request. The DOJ ROB explains that acknowledgment of the DOJ ROB also indicates consent to monitoring, recording, and collection of data on all DOJ devices for law enforcement purposes.

JEFS system is only used as a transport infrastructure and is not designated as an official record-keeping system. Notice and opportunity to consent on individual information that may be contained on the files shared is governed by the various authorities delineating Component

missions and authorizing the collection and maintenance of information to carry out such missions.

Moreover, as noted above, JEFS is a transport infrastructure and because of the varied nature of the Department's work, the files shared via the JEFS system could conceivably include any type of SBU Moderate information. However, to the extent that content contained in such communications are protected by federal law, including the Privacy Act, notice is provided by various DOJ Privacy Act systems of records notices (SORNs), which apply depending on how information is retrieved. These notices and documents are published in the Federal Register and available to the general public, as described in Section 7, below.

Finally, a link to the Department of Justice Website Privacy Policy is displayed in the footer of every page in the JEFS system.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: May 27, 2015 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The Box SaaS has a FedRAMP authorization[15] at the Moderate Impact level. Box utilized a FedRAMP Third-Party Assessment Organization (3PAO) to perform an independent security assessment against a FISMA moderate security baseline. JEFS has a security categorization of Moderate. The identified DOJ security controls have been tested and implemented to protect against risks identified in the security risk assessment which includes those listed in DOJ Security Assessment and Authorization Handbook v. 8.4, providing the framework and direction for performing security assessments and authorizations of all DOJ IT systems, as well as those listed in response to question 6.2. The Justice Management Division, Service Delivery Staff, Application and Web Services Staff is responsible for maintaining the enterprise security Authorization To Operate (ATO) of JEFS. To leverage the JEFS enterprise ATO, Components sign the JEFS Memorandum of Agreement and adhere to the ATO and associated Standard Operating Procedures.

[15] The Federal government's FedRAMP program provides a "cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies." More information on the FedRAMP program can be found at: https://www.fedramp.gov.

X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: DOJ IT security standards, which include monitoring, testing, and evaluation requirements, have been applied to the system. The security controls for JEFS are assessed and/or reviewed annually at a minimum, using the Cyber Security Assessment and Management application, to include all three classes: management, operational, and technical. The assessment and review/update is documented in said system. See the response to question 6.2 for additional information on monitoring, testing, and evaluation.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: JEFS provides reporting and audit trail of account activities on both user accounts and files. Audit logs can only be accessed by authorized staff as required to ensure compliance with security requirements. The JEFS system does not collect data on the content of the files shared. The JEFS system has application access controls that limit access to files and folder using role-based permissions to safeguard against unauthorized access, use, and disclosure of information.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	Other (specify): As further defined by each DOJ Component.

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The following access and security controls have been utilized to protect privacy and reduce the risk of unauthorized access and disclosure:

- JEFS has a security categorization of FISMA Moderate. The Box SaaS has a FedRAMP authorization at the Moderate Impact level. DOJ has assessed and implemented all applicable security controls that are the DOJ responsibility for a FISMA Moderate baseline.

- The JEFS system is accessible to DOJ employees, contractors, and approved users from external entities outside DOJ, only when approved by the DOJ Component Authorizing Official or designee. Additionally, some Components impose further requirements that must be met prior to granting a JEFS account.

- JEFS has specific controls in place that ensure users can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions

associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, JEFS uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed; and that the user is restricted to the authorized type of interaction with the specific files or folders.

- In JEFS, every file is encrypted in transit with high-grade SSL encryption compliant with FIPS 140-2. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. All physical co-location facilities used as the primary processing facilities are located within the United States. The cloud service provider personnel can see the encrypted files and metadata about those files, such as the file create date, but not the information within the files themselves.

- To protect privacy and reduce the risk of unauthorized access and disclosure, the JEFS system has automated functionality to place files that may contain SSNs or files with words/phrasing similar to security markings higher than SBU (e.g. Top Secret) into a restricted "Quarantine" area. The files will then require action from a JEFS Administrator before they become available for use.

- All users must complete CSAT annually, as well as read and agree to comply with DOJ Information Technology Rules of Behavior and the JEFS Terms of Usage, prior to accessing the JEFS system and annually thereafter. Additionally, JEFS administrators must complete JEFS Administrator training, which includes JEFS security training.

- JEFS is configured with automatic audit logging which includes logging of JEFS Administrator activity. Further, logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. JEFS audit logs can only be accessed on read-only mode by authorized DOJ JEFS users with privileged access. JEFS audit logs are automatically monitored by the Box SIEM tool, which would flag any alteration of JEFS audit logs.

- Responses to potential unauthorized disclosures or data breaches are covered in vendor contracts and system rules of behavior in order to ensure appropriate procedures and reporting.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created or has been created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • JUSTICE/DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009), and modified at 82 Fed. Reg. 24151, 153 (May 25, 2017); • JUSTICE/DOJ-002, Department of Justice Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 Fed. Reg. 24147 (May 25, 2017); • Other published DOJ system of records notices depending on the nature of information in the communication or collaboration document and how the information is retrieved. These SORNs apply only to the extent of the information for JEFS accounts as described in section 2.1.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

JEFS Administrators can retrieve JEFS user account information and audit log information by user account name or user account email address.

JEFS has built controls that ensure every user can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, JEFS uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed; and that the user is restricted to the authorized type of interaction (e.g. read-only) with the specific files or folders.