Criminal Division

Privacy Impact Assessment
for the
CLOUD Act Case Management & Data Retrieval Systems

Issued by:
Jennifer A.H. Hodge
Criminal Division, Senior Component Official for Privacy

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

Date approved: January 21, 2021

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[1] among other enactments, modernizes federal law to address evolving internationally diversified data storage practices and cloud computing. The CLOUD Act provides an alternative to mutual legal assistance requests by permitting the United States and eligible foreign countries to enter into bilateral executive agreements (CLOUD Act Agreements) to more efficiently obtain electronic evidence related to the prevention, detection, investigation, or prosecution of serious crime. The CLOUD Act also provides the domestic legal authority necessary to implement such agreements, including removing U.S. law restrictions such that communications service providers (CSPs) can comply with lawful foreign orders for electronic data that are covered by a CLOUD Act Agreement. The agreements facilitate each party's access to certain electronic communications data stored by or accessible to CSPs that are subject to the laws of the other party, for purposes of countering serious crime.

In order to manage the United States Department of Justice's (Department or DOJ) role in these CLOUD Act Agreements, the Department's Criminal Division (Division), Office of International Affairs (OIA) is developing a new information system named CLOUD to document and manage the lifecycle of orders subject to CLOUD Act Agreements (CLOUD Act Orders). CLOUD consists of a case management system and a data retrieval system. The Division conducted this Privacy Impact Assessment to assess and mitigate the risks to the Personally Identifiable Information (PII) collected in this system, which includes but is not limited to names, e-mail addresses, mobile phone numbers and electronic account information for system users. Additionally, documents transferred through CLOUD may include significant quantities of personal information relating to the substantive work of the Department as well as state, local, and territorial law enforcement. Because of the varied nature of these law enforcement agencies' work, documents transferred through this system of information could conceivably include almost any type of unclassified PII.

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.

Both the U.S. and foreign governments increasingly seek access to electronic data held by service providers that may be located outside of their territorial boundaries or subject to more than one country's laws. Such data is often critical to investigations of serious crime by authorities around the world, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime. While the United States has faced serious issues in accessing such information to protect public safety, the need is even greater for foreign government partners, because so much information is held by companies based in the United States. In recent years,

[1] Pub. Law. No. 115-141, 132 Stat. 348, 1213 (2018) ("the CLOUD Act") (codified at 18 U.S.C. § 2523), https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf.

the number of mutual legal assistance treaty (MLAT) requests seeking electronic evidence from the United States has increased dramatically, straining resources and slowing response times. Foreign governments have repeatedly expressed a need for increased speed in obtaining this evidence. In addition, many of the assistance requests received by the U.S. seek electronic information related to individuals or entities located outside the U.S., and the only connection to the investigation is that the evidence happens to be held by a company based in the U.S.

The CLOUD Act establishes a domestic legal framework under which the proposed agreements can facilitate direct cross-border access to data. Specifically, the CLOUD Act authorizes the United States to enter into agreements with foreign governments who meet the Act's rigorous requirements with respect to human rights and rule of law protections. In addition, it amends provisions of the Wire and Electronic Communications Interception and Interception of Oral Communications Statute (Wiretap Act), 18 U.S.C. §§ 2510-2522, the Pen Registers and Trap and Trace Devices Statute (Pen/Trap Statute), 18 U.S.C. §§ 3121-3127, and the Stored Wire and Electronic Communications and Transactional Records Access Act (SCA), 18 U.S.C. §§ 2701-2713, to lift U.S. legal restrictions on CSP disclosures to the partner government for the purpose of responding to an Order subject to a CLOUD Act Agreement. The CLOUD Act requires that the partner government must also reciprocally lift any of its legal restrictions on similar CSP disclosures in response to lawful orders under the agreement from authorities in the United States.

The CLOUD Act provides that the U.S. may enter into CLOUD Act Agreements only with rights-respecting countries that abide by the rule of law. In particular, before the U.S. can enter into a CLOUD Act Agreement, the CLOUD Act requires that the U.S. Attorney General (AG) certify to the U.S. Congress that the partner country has in its laws, and implements in practice, robust substantive and procedural protections for privacy and civil liberties, based on factors such as:

- adequate substantive and procedural laws on cybercrime and electronic evidence, such as those enumerated in the Budapest Convention;
- respect for the rule of law and principles of nondiscrimination;
- adherence to applicable international human rights obligations;
- clear legal mandates and procedures governing the collection, retention, use and sharing of electronic data;
- mechanisms for accountability and transparency regarding the collection and use of electronic data; and
- a demonstrated commitment to the free flow of information and a global Internet.

To date, the U.S. has entered into a CLOUD Act Agreement with the United Kingdom of Great Britain and Northern Ireland. Additional agreements are under discussion with other countries. U.S. authorities intend that the U.S. interests outlined in the existing Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, October 3, 2019 (U.S.-UK Agreement), and the framework and processes outlined within that Agreement, will remain essentially the same for new agreements with other, trusted countries. The language in new CLOUD Act Agreements may vary slightly to accommodate different negotiating partner needs, such as including assurances regarding the use of CLOUD Act Agreement-derived data. The ability to document such requirements will

be built into the CLOUD case management system as they are encountered. However, the agreements should not initiate the addition of a new PII collection type within the case management system.

As set forth in the U.S.-UK Agreement, CLOUD Act Agreements concern data stored or processed by private entities (Covered Providers), to the extent that the entity (1) provides to the public the ability to communicate, or to process or store computer data, by means of a computer system, or telecommunications system; or (2) processes or stores certain electronic or wire communications on behalf of such a private entity. Such data (Covered Data) may include the contents of electronic or wire communications, non-content information associated with such communications, and subscriber information. CLOUD Act Agreements provide that the Issuing Party[2] may issue an Order[3] seeking Covered Data[4] from a foreign Covered Provider,[5] provided that the Order is in compliance with the Issuing Party's domestic laws, the alleged offense qualifies as a Serious Crime,[6] the Order invokes the Agreement between the appropriate countries, and the Order meets all other requirements set forth in the Agreement. Each party's Designated Authority will be responsible for reviewing and certifying that each Order complies with the relevant CLOUD Act Agreement. The Designated Authority will also be responsible for transmitting the Order to the Covered Provider and notifying the Covered Provider that the relevant CLOUD Act Agreement has been invoked as to that Order. In response, the Covered Provider may then provide the responsive Covered Data directly back to the Issuing Party's Designated Authority. Covered Providers receiving Orders issued under CLOUD Act Agreements may raise specific objections to the Orders first with the Issuing Party's Designated Authority, and ultimately with the Receiving Party's Designated Authority. Should such objections be raised, the Parties may confer in an effort to resolve any such objections. If the Receiving Party's Designated Authority concludes that the Agreement may not be properly invoked with respect to any Order, it will notify the Issuing Party's Designated Authority and the relevant Covered Provider of that conclusion, and the Agreement will not apply to that Order.

As the Designated Authority for the U.S. under the U.S.-UK Agreement, as well as future CLOUD Act Agreements, OIA is responsible for confirming the validity of, transmitting, and managing the responses to Orders sought by federal, state, local, or territorial authorities (U.S. Issuing Agencies) for transmission under the Agreements. OIA is also responsible for addressing any concerns about those Orders with foreign Covered Providers and, if necessary, foreign Designated Authorities, and for addressing objections from U.S. Covered Providers related to Orders received from foreign Designated Authorities. OIA will manage this process through CLOUD. CLOUD is a two-prong system of information which contains a database application to track, review, document, and facilitate the CLOUD Act Orders, and a secure, walled-off Data Repository (DR), through which responsive data will pass from the Covered Providers to the U.S. Issuing Agencies.

---

[2] This PIA incorporates the definitions stated in the existing U.S.-UK Agreement.
[3] *See id*.
[4] *See id*.
[5] *See id*.
[6] *See id*.

The day-to-day management prong of CLOUD will be performed by the database application named CLOUD Act Support System (CASS). CASS will store a copy of the submitted Order, along with the professional contact information for both the Issuing Agency and the Covered Provider for each Order. CASS will also capture the Issuing Agency's case docket number, the offenses involved, the account identifiers of the Covered Data, date/number of previously issued preservation orders and any special confidentiality needs. Important date/time stamps of entries made in CASS will append to the record as they occur. Using this information, CASS will track and document the lifespan of Orders for Covered Data made by U.S. law enforcement Issuing Agencies, including federal, state, and local authorities, to Covered Providers in a trusted foreign country that is party to a CLOUD Act Agreement. It will also track and document any objections raised to the U.S. Designated Authority by U.S. providers in response to Orders transmitted by foreign Designated Authorities and the resolution of those instances.

To initiate the CLOUD Act process, the Issuing Agency must submit the relevant Order to OIA. Issuing Agencies will e-mail their Order, a signed CLOUD U.S. Issuing Agency Certification of Compliance (Certification), and a certificate showing completion of the required training to a designated CLOUD Act Agreement e-mail address in OIA.[7] That information will then be manually entered into CASS by OIA employees/contractors. The Certification, additional instructions, and a link to the mandatory training can be accessed by authorized users of the National Domestic Communications Assistance Center (NDCAC) portal of the Federal Bureau of Investigation. Eventually, federal prosecutors will have the option to directly enter their Orders to CASS through a data entry screen. These users will create a limited access, entry-only account which allows entry of their Order and related documents, along with mandatory certifications of compliance for each specific legal requirement of the CLOUD Act Agreement, and a certificate showing completion of mandatory CLOUD Act Agreement training. These entry-only users will be able to monitor the progress of their Orders, but their access will be limited to their case only. Initially, the entry-only access will be limited to federal prosecutors, and OIA will evaluate options for expanding entry-only access to state, local, territorial or other federal prosecutors (such as military).

Regardless of entry method, in order to ensure compliance with the CLOUD Act Agreements, each Issuing Agency must certify that the conditions set forth in the applicable agreement have been met. The Issuing Agency must also certify that it will comply with audits conducted by the U.S. Department of Justice as to compliance with the Agreement and U.S. Targeting Procedures, and will timely provide the information requested in connection with that audit. Once received, OIA will review each Order in the capacity of the U.S. Designated Authority. Each Order and submission attachments will be reviewed by an attorney who is a subject-matter expert for legal validity of, and compliance with, the applicable CLOUD Act

[7] CRM will utilize appropriate safeguards to protect the transmission of all personally identifiable information commensurate with the sensitivity of the data at risk. This includes the implementation of secure ways, consistent with the Department's evolving systems and practices with regard to e-mail, to transfer DOJ information via e-mail communications. The CRM Senior Component Official for Privacy, along with OPCL, DOJ OCIO, and appropriate CRM personnel, will review the security of these transmissions to determine whether current safeguards appropriately protect the information or whether improvements are needed.

Agreement. The assigned attorney will work with the Issuing Agency to gather any additional information to ensure that the Order complies with the relevant Agreement, if needed, and ultimately submit a recommendation to the Associate Director of OIA. The Associate Director will issue the final approval or denial decision on behalf of the U.S. Designated Authority. If the Associate Director determines that the Order meets all applicable requirements, the Order and a certificate issued by the Designated Authority invoking the CLOUD Act Agreement as to that Order will be transmitted to the Covered Provider.

The second prong of the CLOUD Act Case Management & Data Retrieval Systems is DR, a secure information portal through which Covered Providers may choose to provide responsive Covered Data in response to Orders. DR is an independent Division-managed information system, with independently controlled security protocols. It will be authorized to permit upload-only access to foreign personnel and individuals who have not completed the appropriate background assessment. This will allow the system to receive data from necessary foreign entities. CASS and DR will not communicate directly. In order to expedite deployment of this system, initially, OIA users will manually enter trigger-dates into CASS, such as when a Covered Provider enters Covered Data into DR, or when the Issuing Agency has subsequently downloaded the Covered Data.[8]

DR is a separate occurrence of the Justice Enterprise File Sharing System (JEFS system), owned by the Justice Management Division and administered by the Criminal Division. For purposes of this assessment, this PIA fully incorporates the Departmental JEFS PIA,[9] unless otherwise noted within this PIA. 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. The DR occurrence of JEFS is authorized to operate by the Department Chief Information Officer (CIO). The CIO and the Department Security Officers (DSO) have waived the standard Department restriction against foreign personnel access to enable granting limited access to foreign nationals in the role of the point-of-contact for foreign Covered Providers.

Once the Issuing Agency and Covered Provider have completed their required certifications and an account is approved by the Division Approving Authority, access controls involving both the specific transaction and use limitations will be set by OIA personnel in DR. This will limit the parties involved to their designated role (uploading or downloading of information) and control the transaction. When OIA receives the notification that a Covered Provider has uploaded their responsive Covered Data into DR, OIA will notify or cause notification to be sent to the designated point-of-contact for the Issuing Agency, to download the data. If Covered Data is not downloaded within 30 days, the Issuing Agency will receive a reminder notice. At the expiration of the 60-day period (either from date of upload or date of last viewing), all data pursuant to the Order will be automatically deleted from DR and maintained only in the Issuing Agency's case file. An additional, by request only, emergency seven (7) day recovery of deleted files can be performed in DR.[10]

---

[8] A secure method of communicating the pertinent dates between CASS and DR is under development and will be integrated shortly.
[9] The JEFS PIA can be accessed here: https://www.justice.gov/jefs_pia/download.
[10] Under limited, case-by-case circumstances, the JEFS System Owner, in consultation with the DOJ Office of the Chief

In the normal course of business, neither OIA nor Division IT personnel/contractors will access or view the documents passing through DR. However, a limited number of OIA employees/contractors and Division IT personnel/contractors will have the ability to access the documents in order to address unforeseen technical or document quality issues, should the need arise.

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	Clarifying Lawful Overseas Use of Data Act (Cloud Act), PL 115-141[11] 5 U.S.C. § 301; 44 U.S.C. § 3101
☐ Executive Order	
☒ Federal Regulation	Delegation memo designating OIA as the U.S. authority responsible for executing CLOUD Act agreements, estimated to receive final approval in August 2021.
☒ Memorandum of Understanding/agreement	Memorandum of Understanding between the Department of Justice, Office of the Chief Information Officer and the Division regarding the use of JEFS dated July 1, 2020
☒ Justice Manual[12]	Departmental Guidance is under development and the review and approval process is anticipated to be completed by the fall of 2021.

Information Officer, Cybersecurity Services Staff, may grant a waiver to extend the 60-day retention period.

[11] *See supra* note 1.

[12] https://www.justice.gov/jm/justice-manual.

☒ Other (summarize and provide copy of relevant portion)	Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, October 3, 2019.[13] Future Executive Agreements, as enacted pursuant to the CLOUD Act 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

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.

[13] See *supra* note 2.

(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 & D	Professional Information for both the Issuing Authority and the Covered Provider; Categories 1 and 2 (description at bottom of chart)*
Professional Contact Information	X	A, B, C & D	Professional Information for both the Issuing Authority and the Covered Provider; Categories 1 and 2
Account Identifiers	X	C & D	Categories 1, 2, and 3
Date of birth or age	X	C & D	Categories 1 and 2
Place of birth	X	C & D	Category 1
Gender	X	C & D	Category 1
Race, ethnicity or citizenship	X	C & D	Category 1
Religion	X	C & D	Category 1
Social Security Number (full, last 4 digits or otherwise truncated)	X	C & D	Categories 1 and 2
Tax Identification Number (TIN)	X	C & D	Categories 1 and 2
Driver's license	X	C & D	Categories 1 and 2
Alien registration number	X	C & D	Categories 1 and 2
Passport number	X	C & D	Categories 1 and 2
Mother's maiden name	X	C & D	Category 1
Vehicle identifiers	X	C & D	Categories 1 and 2
Personal mailing address	X	C & D	Categories 1 and 2
Personal e-mail address	X	C & D	Categories 1 and 2
Personal phone number	X	C & D	Categories 1 and 2
Medical records number	X	C & D	Categories 1 and 2
Medical notes or other medical or health information	X	C & D	Category 1
Financial account information	X	C & D	Categories 1 and 2
Applicant information	X	C & D	Category 1
Education records	X	C & D	Category 1
Military status or other information	X	C & D	Category 1
Employment status, history, or similar information	X	C & D	Category 1
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	Category 1

(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	C & D	Category 1
Legal documents	X	C & D	Category 1
Device identifiers, e.g., mobile devices	X	C & D	Categories 1 and 2
Web uniform resource locator(s)	X	C & D	Category 1
Foreign activities	X	C & D	Category 1
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Category 1
Juvenile criminal records information	X	C & D	Category 1
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	Category 1
Whistleblower, e.g., tip, complaint or referral	X	C & D	Category 1
Grand jury information	X	C & D	Category 1
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C & D	Category 1
Procurement/contracting records	X	C & D	Category 1
Proprietary or business information	X	C & D	Categories 1 and 2
Location information, including continuous or intermittent location tracking capabilities	X	C & D	Category 1
Biometric data:	X	C & D	Category 1
- **Photographs or photographic identifiers**	X	C & D	Category 1
- **Video containing biometric data**	X	C & D	Category 1
- **Fingerprints**	X	C & D	Category 1
- **Palm prints**	X	C & D	Category 1
- **Iris image**	X	C & D	Category 1
- **Dental profile**	X	C & D	Category 1
- **Voice recording/signatures**	X	C & D	Category 1
- **Scars, marks, tattoos**	X	C & D	Category 1
- **Vascular scan, e.g., palm or finger vein biometric data**	X	C & D	Category 1
- **DNA profiles**	X	C & D	Category 1
- **Other (specify)**	X	C & D	Category 1
System admin/audit data:			
- **User ID**	X	A, B, C & D	
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	x	A, B, C & D	
- **Queries run**			
- **Content of files accessed/reviewed**	x	A, B, C & D	

(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
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	C-D	Category 1

*Category 1: This information may be captured and transmitted in non-indexed form through DR based on the broad range of information types that may be contained within the responsive data.

*Category 2: Although not specifically solicited, this information may be captured in CASS in non-indexed form via the submitted Order.

*Category 3: This is a required data field for CASS.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

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

Government sources		
☒ Within the Component	☒ Other DOJ components	☒ Other federal entities
☒ State, local, territorial	☒ Foreign	
☐ Other (specify):		

Non-government sources		
☐ Members of the public	☐ Public media, internet	☐ Private sector
☐ Commercial data brokers		
☒ Other (specify):	Foreign Covered Providers	

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	☒	☐	☒	Issuing Agencies will e-mail their initial Order and other information to a designated DOJ e-mail address. The information will then be manually entered into CASS. Eventually, Issuing Agencies will be able to create a submission-only account in CASS in order to upload their initial Order. Disclosures will be made on a case-by-case basis to the designated point-of-contact for the Issuing Agency in DR via an access and transaction-controlled account. Finally, information may be accessible to DOJ entities for auditing and accountability reviews.
DOJ Components	☒	☐	☒	
Federal entities	☒	☐	☒	
State, local, territorial gov't entities	☒	☐	☒	
Public	☐	☐	☐	
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☐	☐	☐	
Private sector	☐	☐	☐	
Foreign governments	☒	☐	☐	Case-by-case disclosure of certain case-related information, including copies of the applicable Order, to the foreign government in instances where the foreign government is arbitrating a dispute over the application of the relevant CLOUD Agreement to the Order for data held by a foreign-based Covered Provider.

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.**
Foreign entities	☒	☐	☒	Case-by-case disclosures of the Order Document and their account identifiers will be provided to the designated point-of-contact for Covered Providers on a need-to-know basis. They will be issued an access and transaction-controlled account to provide responsive information.
Other (specify):	☒	☐	☐	Reports to officials outside DOJ (e.g., Congress) concerning Division caseload, activities, performance, and needs.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

This information will not be released to the public for "Open Data" purposes.

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.

Individuals are provided with general notice of the existence of case files through the SORNs;[14]

DOJ/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017).

[14] Unlike the JEFS PIA, the Division does not interpret all individuals to be fully informed of the specific collection of information about the individual on whom the records pertain. Although users of the system are made aware of the system operation and audit log data collection of the system in a manner consistent with the JEFS PIA, the subjects of information contained in the documents passing through DR are not individually informed of the information sharing conducted by this system due to operational security needs.

JUSTICE/DOJ-002, Department Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec.30, 1999) and amended at 82 Fed. Reg. 24147 (May 25, 2017).

JUSTICE/DOJ-014, Department 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).

The above listed SORNs provide the necessary notice to the public, as required by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a (2018). To provide the public with more detailed information on the collection, use, maintenance, and dissemination of CLOUD Act records, the Criminal Division will review its existing data practices in CLOUD and determine whether it is in the Department's interest to create a new System of Records Notice.

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 are provided with general notice of the existence of case files through the System of Records Notice, Central Criminal Division Index File and Associated Records, JUSTICE/CRM-001 DOJ Computer Systems Activity and Access Records, DOJ-002 Department Computer Systems Activity and Access Records, and DOJ-014 Department of Justice Employee Directory System.

Generally, individuals are not provided with specific or direct notice of collection about themselves, as it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

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.

Information in this system is exempt from the access, amendment, correction, and notification procedures of the Privacy Act. Individuals may make access requests, or the information maintained in this system via the Freedom of Information Act (FOIA). Such requests will be processed according to the provisions of the FOIA.

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): For security compliance purposes, CASS is an application of the Custom Database Application System (CDAS), for which the current ATO expires on October 23, 2021. Data Repository is a separate occurrence of the JEFS system, owned by the Justice Management Division and administered by the Division. JEFS operates on a continuous ATO. **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:** All ATO process and risk assessment materials, including the existence of POAMs resulting from those processes are recorded in the Justice Management Division CSAM records for the DR, CDAS and CASS system. This information is normally considered Information System Vulnerability Information and is controlled by the relevant Information System Security Officer.
	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:** As a sub-system of CDAS, CASS has undergone assessments, penetration tests, vulnerability scans, and is monitored by the Division Information Systems Security Officer. As a separate occurrence of the JEFS system, DR has undergone assessments, penetration tests, vulnerability scans, and is monitored by the Justice Management Division Information Systems Security Officer.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The Division collects logs according to the standards in the DOJ CyberSecurity Standards, which include Operating System, Web, Database and Application logs for every FISMA-applicable system. Logs are correlated into appropriate DOJ information systems managed by JMD. Access to these logs is provided to the Justice Security Operations Center, who provided security analysis and log monitoring for unusual activity based on the algorithms and analysis that they provide. Information Owner/Stewards that identify additional audit review requirements per the NIST control selections in their System Security Plan and further defined by entries in a Continuous Monitoring Implementation Plan (CRM Template) may have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the business/information owner.

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 OIA employees/contractors working on CLOUD Act Orders receive internal training on the legal and technical requirements. All personnel seeking to submit Orders to be transmitted under the Agreement as an Issuing Agency must complete and certify completion of mandatory CLOUD Act training provided online by the National Domestic Communications Assistance Center (NDCAC)[15] before an Order will be considered for transmission.

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?

All Division systems implement technical security to reduce the risk of compromise to PII information. Specifically, certain access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- Both CASS and DR have a security categorization of FISMA Moderate and has selected the applicable security controls for a Moderate baseline.
- The CASS Application is accessible by OIA employees and contractors only and utilizes tiered/role-based access commensurate with the end-user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to perform the job, and is individually verified through the employee's PIV card.
- CASS is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- As described throughout this PIA, all CASS users must complete annual CSAT training, as well as read and agree to comply with DOJ information technology Rules of Behavior. CLOUD system administrators must complete additional professional training, which includes security training.
- DR users agree, at least annually, to the JEFS Terms of Usage that include General Rules of Behavior and the DOJ Website Privacy Policy.
- Audit logging is configured, and logs are maintained to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized

[15] https://ndcac.fbi.gov/.

access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.

Overall, the CLOUD Act Case Management & Data Retrieval System defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

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.)

Disposition of records within the CLOUD Act Case Management & Data Retrieval Systems will conform to processes and procedures established by the Division Records Management Section (RMS) for the disposition of softcopy records. A records retention schedule is currently under development. DR transactions will comply with the JEFS record retention requirements as described in the JEFS PIA.

The National Archives and Records Schedule is under development. It is anticipated that the case files maintained in CASS related to CLOUD cases will be retained for a period of 25 years.

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. ☒ 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:

System of Records Notice JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017).

DOJ-002, DOJ Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec.30, 1999) and amended at 82 Fed. Reg. 24147 (May 25, 2017)

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)

The above listed SORNs provide the necessary notice to the public, as required by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a (2018). To provide the public with more detailed

information on the collection, use, maintenance, and dissemination of CLOUD Act records, the Criminal Division will review its existing data practices in CLOUD and determine whether it is in the Department's interest to create a new System of Records Notice.

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.***

Privacy Risk: Noncompliance with the U.S. principals of privacy protection

Mitigation: The overarching premise of the CLOUD Act is to ensure U.S. privacy and civil liberty interests are satisfied while balancing the public-safety need to expedite the flow of investigative information. Beginning with the selection criteria of a partner foreign government, the CLOUD Act requires potential partners to demonstrate a history of respecting the rights of their citizens and abiding by the rule of law. As described above, in Section 2.1, the AG must certify to Congress that a country employs privacy and civil liberty laws, practices and protections before a country can be considered a trusted partner. Once that criteria is demonstrated, a country can enter into a CLOUD Act Agreement, which must itself meet the requirements set forth in the CLOUD Act. The AG must, as soon as is reasonably practicable, publish in the Federal Register the certifications and determinations by the AG regarding a CLOUD Act Agreement.[16] U.S. authorities intend that the U.S. interests outlined in the existing United Kingdom of Great Britain and Northern Ireland Agreement, and the framework and processes outlined within it, will remain fundamentally the same in the Agreements with additional trusted countries.

On an individual level, CLOUD Act Agreements and related targeting and minimization procedures hold law enforcement accountable to the mandates of the Agreement by requiring that Orders subject to the Agreement may not generally target Receiving Party Persons (as defined in the applicable Agreement), and by requiring that U.S. Issuing Agencies maintain

[16] *See, e.g.*, U.S. Dept. of Justice, Clarifying Lawful Overseas Use of Data Act; Attorney General Certification and Determination, 85 Fed. Reg. 12578 (March 3, 2020) (disclosing the certification and determination of the U.S.-UK CLOUD Agreement).

records available for audit related to Orders subject to the Agreement (all described in Section 2.1). Issuing Agencies must complete mandatory online CLOUD Act training and certify their awareness and intent to abide by the targeting and minimization procedures during the submission process. Following submission, a subject-matter expert attorney in OIA will review the Order and related documentation for appropriate compliance prior to recommending transmission of the Order. OIA attorneys and International Affairs Specialists working with CLOUD Act Orders must also complete mandatory training on the application of the CLOUD Act. Lastly, the objections process outlined in existing and future CLOUD Act Agreements is designed to allow Covered Providers to identify and question whether Orders are appropriately subject to the relevant CLOUD Act Agreement by raising objections to the Issuing Party's Designated Authority, Receiving Party's Designated Authority, or both.

Privacy Risk: Unauthorized access

Mitigation: The Department employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. The CLOUD Act Case Management & Data Retrieval Systems also implement access monitoring, privacy and records controls standardized by the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems, as defined in NIST Special Publication 800-53.

Employee access to CASS is limited based on a need-to-know and further delimited by restrictions which limit users to the minimum access needed. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's Personal Identity Verification (PIV) card and pin number for authentication of Division and U.S. Attorney personnel. It also has been evaluated and authorized to operate according to the risk management framework required by the Federal Information Security Modernization Act of 2014 (FISMA). An audit log is maintained of all user logins and actions. Notification of the monitoring is presented clearly when logging into the system.

Entry-only access to CASS will be provided to those individuals who need to submit Orders for transmission under the CLOUD Act Agreement. This access will limit the Issuing Agency to their own submission(s). They will be unable to view or alter other cases or portions of the database. These individuals must be U.S. law enforcement or prosecutorial personnel. They must complete training on the relevant U.S. Targeting Procedures for the CLOUD Act Agreement and certify their intent to comply with the legal requirements. Before entry-only access is granted, they must be verified as law enforcement or prosecutorial personnel. For Department personnel, this is readily verified through their PIV credentials. Until automated access is stood up for other federal, state, local and territorial law enforcement and prosecutorial personnel, verification will be performed using the existing procedures that OIA employs for MLAT and extradition identity verification. These include e-mail domain verification, interviews with the prosecutor, review and authentication of the attached Order documents and verification that the Order contains the signature of a judge or magistrate.

DR is walled off from other Division IT systems. Thus, DR addresses Departmental security protocols which deny access to foreign officials and individuals without appropriate security

and background assessment to access Departmental information technologies. Therefore CASS is protected from all outside access and the risk of outside access is transferred to the walled-off DR application. CASS and DR will not communicate directly. The DR system is accessible to DOJ employees, contractors, and approved users from external entities outside DOJ, only when approved by the Division Authorizing Official or designee. DR has built-in 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, DR 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. Additionally, DR conducts two factor authorization through Short Message Service texts.

The IT system assessment for both CASS and DR are documented in the DOJ CSAM assessment tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no outside access to this system; administrator access is restricted to the few DOJ employees and contractors who administer the program. Additionally, Issuing Authorities must certify from the onset of submitting an Order that they will comply with audits conducted by the U.S. Department of Justice as to compliance with the Agreement and U.S. Targeting Procedures, and will timely provide the information requested in connection with that audit (all described in Section 2.1), serving as a palpable deterrent to misuse.

Privacy Risk: Misuse of information

Mitigation: The Department relies heavily on the training of its employees and need-to-know limitations on access to mitigate the possibility of mis-using information. Department employees and contractors must complete annual training regarding handling of PII as part of the Department's Cyber Security and Awareness Training (CSAT), as well as read and agree to comply with DOJ Information Technology Rules of Behavior. This occurs during their orientation upon entering into service with the Department, and annually thereafter. Additionally, OIA has developed and mandates training for employees granted access to CASS.

The CLOUD Act itself stands as a mechanism to control the appropriate use of the information within. Specifically, the CLOUD Act Agreements define the appropriate uses of information obtained pursuant to this system. In addition to the mandated online training regarding the appropriate uses of CLOUD Act Agreement information, Issuing Agencies must certify to each of the tenants of authorized use.

Privacy Risk: Name association with the database

Mitigation: As in most cases where a record associates a person with a criminal investigation, the mere presence of a name in the system can generate the assumption of

involvement with criminal activity or other damage to their reputation. For this reason, there is no automated dissemination of PII from CASS outside of the approved and trained OIA personnel/contractors, Issuing Authorities and Covered providers. Confidentiality requirements are clearly defined and communicated to all parties involved. Any dissemination must be done pursuant to proper authority and management review. Information obtained from this system is considered law enforcement sensitive. Additionally, de-identification of management reporting is practiced in all instances possible.

Privacy Risk: Over-collection

Mitigation: Because criminal investigations and prosecutions are continually evolving endeavors, it is not always possible to know whether collected information will be relevant or necessary as a matter matures. In order to mitigate these concerns, the Division considered the careful minimization of information collection in the design of the CLOUD Act Case Management & Data Retrieval Systems. The customized interface/ submission worksheet that solicits the minimal amount of information required to meet that operational needs. The system does not solicit or index sensitive identifiers such as social security numbers (SSNs), dates of birth, Federal Bureau of Investigation Numbers, Federal Bureau of Prison Numbers or the like. The solicited information is narrowed to the necessary contact information of system users and account identifiers for the subject of the Order.

A vast amount and variety of information can pass through DR. OIA will review the Order and supporting certification of compliance to ensure that the data sought is targeted and specific. Because DR is walled-off from other Division servers, it will never enter OIA's active control. The documents passing through DR are not maintained as a discrete collection of information. In practice, they are never retrieved or viewed by OIA employees who lack the need-to-know what investigation-specific information is ultimately produced. Instead, they pass directly from the Covered Provider to the Receiving Authority. These documents are automatically purged once sufficient time for the Issuing Authority to retrieve their document has passed.

Additionally, DR 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.

Privacy Risk: Erroneous or inaccurate information

Mitigation: Based on the sensitive investigative nature of these records, members of the public cannot enter records directly into the system or access it for review. Information in this system is obtained pursuant to criminal or civil investigations. The Department has a substantial interest in ensuring the accuracy of the information in this system. Both the Issuing Agency and OIA verify the information in CASS as part of the normal procedures associated with day-to-day tasks, which include multiple levels of oversight and review. Every effort is made to diligently review, verify, and correct information from these records.

Because OIA is ultimately acting as an intermediary between the Issuing Agency and the

Covered Provider, OIA must rely on the Issuing Agency to confirm the accuracy of the information provided in the Order. However, OIA does conduct diligent review of the Order and supplemental documentation for indication of inaccuracies during their legal evaluation. Additionally, it is OIA's practice to provide copies of the original Order with the related certificate invoking the CLOUD Act Agreement to ensure the best possible information is received by the Covered Provider.