Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Complete Discovery Source (CDS) Federal Cloud Discovery Service (FCDS) (OS2700)

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 10/21/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary/Complete Discovery Source (CDS) Federal Cloud Discovery Service (FCDS) (OS2700)

Unique Project Identifier: OS2700

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

CDS – Federal Cloud Discovery Services (FCDS)
Complete Discovery Source (CDS) – Federal Cloud Discovery Services (FCDS) performs a set of operations required to progress through the various phases of the discovery process:

- Chain of Custody Tracking
- Data Staging
- Data Filtering
- De-duplication
- Metadata Extraction
- Full Text Extraction
- Exception Handling
- Data Conversion
- Document Review Management
- Document Review
- Redaction and Annotation
- Load File Production

eDiscovery
During the pre-trial phase in a lawsuit, opposing parties can obtain relevant information from each other through the law of civil procedure. As part of the discovery process, opposing parties usually request and exchange ESI's (Electronically Stored Information).

System Description
Complete Discovery Source's Cloud Electronic Discovery Services (FCDS) SaaS platform is a powerful and secure solution for meeting any electronic discovery need. The eDiscovery application Relativity is offered as a single Commercial Off-The-Shelf (COTS) service. CDS has built a segregated physical and logical environment for its FedRAMP FCDS clients. FCDS runs in fully redundant Windows server environments and includes content analysis of underlying proprietary databases with a web-based graphical user interface (GUI), which consists of clustered VMware servers. All client data is stored on servers running in an active/active cluster

configuration. CDS utilizes a series of redundant Cisco firewalls, routers, and switches to manage network traffic. Production equipment is hosted at the Equinix, Inc. data center located in North Bergen, New Jersey. The Failover datacenter is in Washington D.C.
CDS' Relativity application run in a Windows server environment and includes content analysis of underlying databases with a web-based graphical user interface (GUI). The content analysis runs on Dell PowerEdge R710 servers. The database consists of Dell PowerEdge R710 servers running proprietary databases in an active/active cluster configuration.

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

(b) System location
The primary location is the Equinix, Inc. data center located in North Bergen, New Jersey. The Failover datacenter is in Washington D.C.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The CDS-FCDS is a stand-alone system and does not interconnect with systems outside of its boundaries.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
It operates as a standard collection of networking components, servers, workstations, and applications to house and transmit data securely and reliably.

(e) How information in the system is retrieved by the user
Users access data residing on their workstation or on network locations within the usual office automation applications (word processing, spread sheet, data base).

(f) How information is transmitted to and from the system
Information can be copied from location to location if the user has appropriate access rights. Information can be sent via email if it is not sensitive. Information can be sent by a secure file transfer application if the data is sensitive.

(g) Any information sharing conducted by the system
Results from a FOIA or Privacy Act request (e.g. responsive files) may be shared with the original requestor via a means outside of the FCDS and Relativity, and in accordance outlined in the DOC' s FOIA and Privacy Act Regulations.
Additionally, DOC may extract information from the system to share as authorized by law and in accordance with the routine uses outlined in the applicable System of Records Notice (SORN). When sharing such information with external entities, DOC typically does so

pursuant to non-disclosure agreements, court-approved protective orders, contract provisions regarding privacy and security, or similar data protection controls. These external entities will have no web-based or other online access to the system.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- The Federal Administrative Procedure Act. as amended (Pub. L. 79-404, 60 Stat-237 (1946), 5 U.S.C. Subchapter 11 §§ 551 et. seq.)
- The Freedom of Information Act (FOIA) (5 U.S.C. § 552, as amended; 15 C.F.R. § 4
- The Privacy Act of 1974 (5 U.S.C §552a, as amended; 15 C.F.R. § 4b)
- Departmental Organization Order (DOO) 20-31

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Included in these functions is overseeing the implementation of Departmental policies and procedures for the administration of FOIA and the Privacy Act, including managing the Department's FOIA and Privacy Act request process for providing public access to Departmental records and information. Included in responsive records or files considered for release may be information related to a specific request but not outlined above. Of note, per DOC policy, sensitive information, including sensitive PII, is prohibited from transmittal via unencrypted email mechanisms.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email	X		
Other (specify): Information is derived from existing documents, emails, and other files and records in relation to a request under the FOIA or Privacy Act. As such, information may be collected through a variety of means and mechanisms from the individual to whom it pertains at the original point of collection.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify): Information is derived from existing documents, emails, and other files and records in relation to a request under the FOIA or Privacy Act. As such, information may be collected through a variety of means and mechanisms, including government sources, at the original point of collection.					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Information is derived from existing documents, emails, and other files and records in relation to a request under the FOIA or Privacy Act. As such, information may be collected through a variety of means and mechanisms, including non-government sources, at the original point of collection.					

2.3 Describe how the accuracy of the information in the system is ensured.

Information, including PII, included in the source documents is not checked for accuracy in relation to its use in FCDS. This information is subject to reviews for accuracy and timeliness in accordance with the purpose or activity for which they were originally collected. Additionally, information incorporated into the FCDS system is subject to appropriate security and chain-of-custody controls. In addition to protecting against unauthorized access, alteration, or dissemination, these controls reduce the risk of loss and assure the integrity of information in the system.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII that is collected, maintained, or disseminated will be used. Indicate if the PII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII and maintained and processed by the system is used in administration of FOIA and the Privacy Act by the DOC. The PII identified in Section 2.1 can pertain to federal employees, contractors, and other staff, member of the public, foreign nationals, visitors, or any other party included in the source files that are responsive to a FOIA or Privacy Act request. Of note, per DOC policy, sensitive information, including sensitive PII, is prohibited from transmittal internally and externally via unencrypted email mechanisms.

To the extent that a FOIA request is the subject of litigation, information included in the system may be used as is relevant to the matter which is the subject of litigation.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit 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.)

There is always the potential for insider threat. All DOC employees, including those that maintain this application, are required to take annual cybersecurity and privacy awareness training. There is a risk associated with the inappropriate use of or failure to protect information in FCDS. There is a risk that PII, including sensitive PII, could be misused, lost, or otherwise compromised. DOC has implemented controls which limit access to and use of the system to those Office of the Secretary (OS) employees with a clearly defined need-to-know the information.

FCDS audits successful and unsuccessful logon attempts and user activity in the system. These audits include account management events, policy change, privilege use, data access, data deletions, data changes, permission changes, and all administrator activity. Additionally, CDS contract staff are required to sign a non-disclosure agreement with the Department which outlines their responsibilities in protecting sensitive information, including PII. Finally, training is provided to end-users of the system.

There is a risk that the aggregation and "connection" of multiple documents and other files using metadata, as well as the enhanced search capabilities of the system will create new information about individuals. Because information in the system is derived from existing information or documents within and across DOC systems, the combining and centralizing of such information for the purposes of administering the FOIA and Privacy Act poses little risk to individual's privacy. Similar capabilities already exist within the systems which currently house such information.

Finally, all responsive documents generated because of the processes conducted in FCDS are redacted, in accordance with FOIA and Privacy Act procedures, for sensitive information including PII.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII in the IT system and how the PII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		X
DOC bureaus	X		X

Federal agencies	X		
State, local, tribal gov't agencies	X		
Public	X		
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII.
	No, the bureau/operating unit does not share PII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII. Provide the name of the IT system and describe the technical controls which prevent PII leakage: *FCDS has no interconnections to DOC systems, however, information from DOC systems authorized to process PII may be transferred via secure means (SFTP or portable media) to the system.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII.

6.4 Identify the class of users who will have access to the IT system and the PII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII 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 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: The Privacy Act Statement for the collection and use of information necessary to grant system access is available to users on the form submitted for system access. The Privacy Act notice for the original source collection of records included in the system is presented at the original point of collection or via the relevant System of Records notice as outlined in Section 9.	
X	Yes, notice is provided by other means.	Specify how: Notices may be provided directly to individuals impacted by FOIA or Privacy Act requests, at the original point and time of collection for source records.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII.

	Yes, individuals have an opportunity to decline to provide PII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: FCDS does not directly collect PII, rather, it allows for the search and retrieval of responsive, existing DOC records relative to a request under the FOIA or Privacy Act which may contain PII from other source systems or information collections. As such, opportunities to decline to provide information may be presented at the original time and point of collection.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: FCDS does not directly collect PII, rather, it allows for the search and retrieval of responsive, existing DOC records relative to a request under the FOIA or Privacy Act which may contain PII from other source systems or information collections. As such, opportunities to consent to provide information may be presented at the original time and point of collection.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: FCDS does not directly collect PII, rather, it allows for the search and retrieval of responsive, existing DOC records relative to a request under the FOIA or Privacy Act which may contain PII from other source systems or information collections. Therefore, opportunities to access, amend, or correct PII may be available through the source systems from which data is derived, or through means provided under the Privacy Act and as outlined in the applicable SORN.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: This system is only accessible by authorized DOC FOIA personnel
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 3/20/2019 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Records, emails, documentation accessed within relativity are DOC records; customers in this case are DOC offices and operating units

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

FCDS is a FedRAMP authorized solution which has undergone a security risk assessment and received an Authority to Operate (ATO) from the Environmental Protection Agency (EPA). The Department is performing an additional assessment of the system to leverage that authorization. The system is categorized as a moderate system using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems.

FCDS has implemented various technical and administrative controls, in accordance with guidance outlined in NIST 800-53, Rev 4, to secure information processed by and maintained in the system to include:

- Utilizing two (2) geographically diverse data centers with physical access controls (guards, ID badges. entry devices, etc.)
- Maintenance of Federal data separate from non-Federal client data (Community cloud)
- Encryption of data in transit (SFTP) or hand delivery via encrypted hard drives or other portable media.
    - For physical delivery, physical devices are affixed with a unique identifier upon receipt to track physical chain-of-custody of the device. A chain-of-custody log is maintained.
    - For delivery via SFTP, all data uploaded via the CDS SFTP is protected with SSL encryption while in transit. Additionally, data entering the CDS network is subject to anti-virus and anti-malware scans.
- Continuous monitoring of the CDS environment and auditing of application access and use. These audits include account management events, policy change, privilege use, data access, data deletions, data changes, permission changes, and all administrator activity.
- Two-factor authentication for system access by DOC and CDS users. DOC users are limited to accessing the solution through DOC-issued Government Furnished Equipment (GFE).
- Lockout for 3 failed attempts to gain access to the system.
- Lockout is 1 hour or until the password is reset by contacting the CDS Help Desk.
- Session time outs that lock screens of inactive users after 5 minutes (Relativity application).
- Clearly defined and enforced user roles and permissions grant the least amount of access to data in the system as they need to perform their duties.
    - High level functions are limited to administrative users and access to the database is limited to the database administrators.
    - Authentication of internal (CDS) employees includes the use of RSA tokens for each log-in to the system.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT - 5, Freedom of Information Act and Privacy Act Request Records COMMERCE/DEPT - l4, Litigation, Claims, and Administrative Proceeding Records COMMERCE/DEPT - 25, Access Control and Identity Management System Other SORNs may also be applicable, relevant to the source documents and files from which information in the system is derived in response to a FOIA or PA request.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: General Records Schedule (GRS) 14, Information Service Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing	X	Deleting	X

Other (specify):

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII included in documents and files maintained and managed in the system contain direct identifiers, such as full names, unique identifying numbers etc., information which directly identifies individuals of note per DOC policy, sensitive information, including sensitive PII is prohibited from transmittal via unencrypted email mechanisms. As such, no sensitive PII should be included in any emails in the initial pilot program.
X	Quantity of PII	Provide explanation: Large volumes of PII may be included in documents and files maintained and managed in the system.
X	Data Field Sensitivity	Provide explanation: PII included in documents and files maintained in or managed by the system includes information that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to individuals to whom the information pertains or to the Department. As outlined above, per DOC policy, sensitive information, including sensitive PII, is prohibited from transmittal via unencrypted email mechanisms. As such, no sensitive PII should be included in any emails in the initial pilot program.
X	Context of Use	Provide explanation: PII included in documents maintained or managed by the system may be used as part of ongoing litigation involving the Department.
X	Obligation to Protect Confidentiality	Provide explanation: For most PII contained in documents or files maintained in

		or managed by the system, confidentiality is implied at the original time or point of collection from the subject individual, is required by internal DOC or bureau policy or procedure, or social norms, context, and expectations are such that a reasonable person would assume that information provided is confidential in nature or otherwise protected from unauthorized disclosure or use. In some cases, explicit promises of confidentiality are provided.
X	Access to and Location of PII	Provide explanation: Information is maintained and processed in a secured, FedRAMP authorized Community cloud environment and/or locally on secured, encrypted portable media. Access is limited to a limited number of OPOG and OS personnel with a clearly defined business need-to-know the information and access the system, and limited number of system administrators for CDS who maintain and secure the system.
X	Other:	Provide explanation: Data is generally unstructured in nature and disparate across multiple documents and files. Data is encrypted at rest and protected by various mechanisms, to include dual factor authentication for end-users. Resulting responsive documents and records are redacted, in accordance with FOIA and Privacy Act procedures, for sensitive information, including PII. Additionally, per DOC policy, sensitive information is prohibited from transmittal via unencrypted email mechanisms. As such, no sensitive PII should be included in any emails in the initial pilot program, which reduces the overall risk profile of the program.

Section 12: Analysis

12.1 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. Also, describe the choices that the bureau/operating unit 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. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As there is a persistent potential for insider threat, all users are required to take cybersecurity and privacy awareness training. There is a risk that individuals may be unaware that their information is maintained or processed within the FCDS platform or that they may have limited opportunities to consent to the collection and use of their information in the system. Because the FCDS serves as an eDiscovery management solution for already existing documents, records, and files created using information from source systems, some individuals may be unaware, at the original point of collection, that their information is being processed within the FCDS system(s), or may not consent to such processing. In general, this risk is low, because use of the FCDS for eDiscovery does not alter any existing business processes relating to the purposes for which information was originally collected, nor does the system use such information to make decisions about an individual's rights, benefits, or privileges. Individuals are provided opportunities for notice and consent at the original point

than is necessary for executing the intended purpose. PII, including sensitive PII, may appear in documents, records, and other files related to requests for responsive records for a FOIA or Privacy Act request, or in the administration of associated duties by OPOG, and as such, will vary from case-to-case on what PII is included and may change over time. Documents, files, records, and data managed within the system are limited to that which is necessary to fulfill the purpose as outlined in Section 5.1 above only, and controls exist to limit access and use of the system to those with a clearly defined need- to-know, and to monitor system use. By policy, the transmission of sensitive PII by unsecured email is prohibited at DOC, as described in Section 5.2 of this PIA, this includes both internal and external (inbound and outbound) communications. The Department has implemented DLP solution(s) to identify and remove sensitive PII from unencrypted email communications, reducing the overall risk of sensitive PII being included in the system. Finally, the system allows users to redact information, including PII, in accordance with FOIA and Privacy Act procedures and allowances under the relevant statutes and regulations.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.