Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Complete Discovery Source (CDS)
Federal Cloud Discovery Service (FCDS)
(OS2700)

U.S. Department of Commerce Privacy Threshold Analysis
Office of the Secretary/Complete Discovery Source – Federal Cloud Discovery Service

Unique Project Identifier: OS2700

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 data center 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 purpose that the system is designed to serve*

The CDS – Federal Cloud Discovery Services (FCDS) is designed to 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

e) The way the system operates to achieve the purpose

It operates as a standard collection of networking components, servers, workstations, and applications to house and transmit data securely and reliably.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The information are primarily documents and data created by employees in the furtherance of their work objectives.

g) Identify individuals who have access to information on the system

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users.

h) 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).

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and completecertification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

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). *Continue to answer questions and complete certification.*

_____ 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). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

_____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *(Check all that apply.)*

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

_X__ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

__X__ No, this IT system does not collect any BII.

4. Personally, Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__ Yes, the IT system collects, maintains, or disseminates PII about:
(*Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Other Federal Government personnel
__X__ Members of the public

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

__X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Office of Privacy and Open Government (OPOG) Complete Discovery Source. Federal Cloud Discovery Service and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Office of Privacy and Open Government (OPOG) Complete Discovery Source. Federal Cloud Discovery Service and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Kenyetta Haywood Office: OPOG Phone: 202.482.3743 Email: khaywood1@doc.gov Signature: KENYETTA HAYWOOD Digitally signed by KENYETTA HAYWOOD Date: 2021.07.02 12:35:47 -04'00' Date signed: _____	**Information Technology Security Officer** Name: Jerome Nash Office: OS/OESS Phone: 202.482.3186 Email: jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.08.31 13:48:16 -04'00' Date signed: _____
Privacy Act Officer Name: Tahira Murphy Office: OPOG Phone: 202.482.8075 Email: tmurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.21 13:15:48 -04'00' Date signed: _____	**Authorizing Official** Name: Lawrence W. Anderson Office: Office of the Secretary Phone: 202.482.4444 Email: landerson@doc.gov Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.09.01 14:49:43 -04'00' Date signed: _____

Bureau Chief Privacy Officer Name: Maria Dumas Office: OPOG Phone: 202.483.5153 Email: mdumas@doc.gov Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.21 16:42:42 -04'00' Date signed:	