U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
E-Discovery Software System - Cloud (EDSS-C)

Reviewed by: Henry J. Holcombe, 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 Digitally signed by JENNIFER GOODE
Date: 2025.06.20 14:00:24 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO E-Discovery Software System - Cloud (EDSS-C)

Unique Project Identifier: EBPL-LT-01-00

<u>Introduction</u>: System Description

Provide a brief description of the information system.

The E-Discovery Software System - Cloud (EDSS-C) is a commercial Software as a Service (SaaS) implemented with Relativity One for Government. This SaaS provides for the Preservation, Collection, Processing, Review, Analysis, and Production phases of the Electronic Discovery Reference Model (EDRM). Attorneys and litigation support personnel employ the tool in a variety of legal cases to organize and review the larger amounts of Electronically Stored Information (ESI) that are common today. It is also used with some Freedom of Information Act (FOIA) and Privacy Act (PA) requests that have a lot of responsive content to organize. Courts and other judicial bodies are more critical of proper electronic discovery methods and procedures and this tool provides a secure framework and process for performing electronic discovery.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
EDSS-C is a commercial SaaS.

(b) System location
RelativityOne for Government runs in data centers managed and operated by Microsoft Azure Government deployed in the Azure US Gov Virginia region.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
EDSS-C interconnects with the following system:

Identity, Credential, and Access Management - Identity as a Service (ICAM-IDaaS) is an infrastructure information system that provides authentication and authorization service to secure all USPTO enterprise information systems as well as provide audit ability to user activity.

Network and Security Infrastructure System (NSI) is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
The EDSS-C system is a cloud-based web application that allows the litigation support team to ingest and process large collections of documents. During processing, the software will perform document deduplication, create a text index for searching, provides for imaging of documents, and turns everything into individual documents that can be searched, organized and reviewed along with the document metadata. The software provides an interface and functions for the legal staff to search, review, redact, and categorize documents with tags. The documents can then be turned into a production with Bates numbering, or simply exported into native, image, and text formats for further use and handling. This system allows the legal teams to focus on their core competencies in data analysis, collecting the custodian's data, categorizing their documents and automating the review process. The resultant ESI is used in litigation.

(e) *How information in the system is retrieved by the user*
EDSS-C is a web application that allows authorized users to access and view information in the system using a web browser.

(f) *How information is transmitted to and from the system*
EDSS-C users use a web browser to make a Hypertext Transfer Protocol Secure (HTTPS) connection to the web application.

(g) *Any information sharing*
The system helps legal teams to review, tag, and redact specific documents that will later be exported from the system. These exported document productions can then be provided to courts, opposing counsel, FOIA requesters, and others, as necessary.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
The specific programmatic authorities are the Federal Rules of Civil Procedure (FRCP), Equal Employment Opportunity Commission (EEOC), U.S. Merit Systems Protection Board (MSPB), the Freedom of Information Act and the Privacy Act.

(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.

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

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: PII/BII (including SSNs) may be incidentally collected and maintained as a result of an E-Discovery search and collection. PII/BII collected as part of an E-Discovery search may either be redacted and not disclosed to the opposing party in litigation, or produced subject to a protective order entered into by the parties and signed off on by the trier of fact.					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☒	o. Financial Information	☒
b. Maiden Name	☒	i. Place of Birth	☒	p. Medical Information	☒
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☒	k. Telephone Number	☒	r. Criminal Record	☐

e. Age	☒	l. Email Address	☒	s. Marital Status	□
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	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☒	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☒	k. Procurement/contracting records	☒
d. Work Telephone Number	☒	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	☒	c. Date/Time of Access	☒	e. ID Files Accessed	□
b. IP Address	□	f. Queries Run	□	f. Contents of Files	□
g. Other system administration/audit data (specify):					

Other Information (specify)

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	☒		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☒
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☒	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

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

From an administrative perspective, the EDSS-C application has administrative and support staff that function as points of contact whereby customers may directly contact for the administration of information accuracy.

From a technical implementation, USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information.

Access to the system is only assigned to authorized users with specific role-based restrictions, and individuals with access privileges have undergone training, vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

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.
☒	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):			

☒	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): Click or tap here to enter text.			

☒	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/BII 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	☒	To promote information sharing initiatives	☐
For litigation	☒	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/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII 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).

The system includes information from members of the public and other federal employees.

The EDSS-C is used for E-Discovery on legal matters within OGC. The information collected during E-Discovery may include PII/BII related to individual involved in the legal matter. The EDSS-C system enables legal teams to ingest, search, analyze, and produce very large amounts of E-Discovery data using Relativity One for Government's features and functionality. It allows the legal teams to focus on their core competencies in data analysis, collecting the custodian's data, categorizing their documents and automating the review process. The data is used in 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.)

Adversarial entities, insider threats and inadvertent private information exposure is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires Annual Security Awareness Training for all employees as well as policies and procedures documented in the USPTO IT Security Handbook. All USPTO offices adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

All data transmissions are encrypted and requires credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions to government agencies pass through a DMZ before being sent to endpoint servers. SSNs are encrypted while at rest and in transit.

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	□	□
DOC bureaus	□	□	□
Federal agencies	☒	□	□
State, local, tribal gov't agencies	☒	□	□
Public	☒	□	□

Private sector	☒	□	□
Foreign governments	□	□	□
Foreign entities	□	□	□
Other (specify):	□	□	□

□	The PII/BII in the system will not be shared.

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

□	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
□	No, the bureau/operating unit does not share PII/BII 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 and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ICAM-IDaaS All data transmissions are encrypted and requires credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions to government agencies pass through a DMZ before being sent to endpoint servers. SSNs are encrypted while at rest and in transit.
□	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	□	Government Employees	☒
Contractors	□		
Other (specify): The Relativity vendor support team has access to the technical system, but they do not (by default) have access to the data within the system. We can provide them access to specific matters that may contain PII/BII if this access is needed to address a technical problem.			

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.)*

☒	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: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as notice.
☐	No, notice is not provided.	Specify why not:

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The PII/BII information is being collected individual so there is no opportunity for the individual to decline to provide their PII/BII during an E-Discovery collection but not directly from the individual so there is no opportunity for the individual to decline to provide their PII/BII.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The PII/BII information is being collected during an E-Discovery collection but not directly from the individual so there is no opportunity for the individual to consent to particular uses of their PII/BII.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The PII/BII information is being collected during an E-Discovery collection but not directly from the individual so there is no opportunity for the individual to review/update their PII/BII.

Section 8: Administrative and Technological Controls

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

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: PII/BII is monitored, tracked, or recorded via audit logs.
☒	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): 11/8/2024 □ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	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).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
□	Contracts with customers establish DOC ownership rights over data including PII/BII.
□	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
□	Other (specify):

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).*

The system is implemented with encryption (Secure Sockets Layer (SSL)). Authorized users have role-based permissions. Documents are reviewed for PII/BII and content is redacted before making it available to the individual requesters.

The USPTO uses continuous monitoring to ensure that security controls are in place. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security and Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the enhanced system. Additional management controls include performing background checks on all personnel, including contractor staff.

A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for EDSS-C and this informs the security controls applied to the system.

Manual procedures are followed for handling extracted data containing sensitive PII. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

- Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.

- Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
- Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private Network (VPN).
- Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

Section 9: Privacy Act

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

☒ 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."

☒	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-14: Litigation, Claims, and Administrative Proceeding Records EEOC/Gov-1: Equal Employment Opportunity in the Federal Government Complaint and Appeal Records MSPB/Gov-1: Appeals and Case Records Commerce/Dept-5: Freedom of Information Act and Privacy Act Request Records Commerce/Dept-18: Employee Personnel Files Not Covered by Notices of Other Agencies
☐	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.)*

☒	There is an approved record control schedule.

	Provide the name of the record control schedule: GRS 5.2, Item 020, Intermediary 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:
☒	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	☐
Degaussing	☐	Deleting	☒
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.
☒	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.)*

☒	Identifiability	Provide explanation: The combination of name, address, email, and phone can be used to identify a particular individual.
☒	Quantity of PII	Provide explanation: There are about 10 employment matters in EDSS-C each year involving individuals that may PII content. There are about 8 FOIA/PA requests in EDSS-C each year may that may contain PII. There are about 4 IP litigation cases in EDSS-C each year that may contain BII. There is no reasonable way to estimate the amount of PII/BII that may be contained in each of these matters.
☒	Data Field Sensitivity	Provide explanation:

		The PII is found on documents and is not stored in data fields.
☒	Context of Use	Provide explanation: E-Discovery content is used in legal matters. Attorneys and litigation support personnel employ the tool in a variety of legal cases to help and organize the larger amounts of Electronically Stored Information (ESI) that are common today. It is used to initiate Litigation Holds to identify and preserve the ESI; collect, process, and analyze the information; redact, assemble and export relevant information and reports.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: PII is found in some E-Discovery content and is only accessible to authorized individuals. PII is redacted and not disclosed.
☐	Other:	Provide explanation:

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.)

In addition to insider threats, activity which may raise privacy concerns include the collection, maintenance, and dissemination of PII in the form of personal and work-related data such as name, telephone number and email address as well as user ID and date/time access etc. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

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:
☒	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:
☒	No, the conduct of this PIA does not result in any required technology changes.