Civil Division

Privacy Impact Assessment for
the
Civil RelativityOne (CRO)

Issued by:
Brian Flannigan
Senior Component Official for Privacy

Approved by: Peter A. Winn
Acting Chief Privacy & Civil Liberties Officer
U.S. Department of Justice

Date approved: October 7, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Civil Relativity One (CRO) is a FedRamp authorized Software-as-a-Service (SaaS) eDiscovery platform, which allows the Division's litigation staff and contractors to collect and preserve; process, review, and analyze, as well as produce and present electronic discovery material for investigative and litigation matters. CRO provides enhanced integrated automation across the electronic discovery review process, which greatly improved processing times. CIV also uses CRO for processing records responsive to some Freedom of Information Act (FOIA) or Privacy Act requests. Finally, CRO houses a workspace dedicated to Victims' Compensation Fund (VCF) cases, including witness statements to serve as both a repository and medium for review.

CRO is deployed as RelativityOne Government, a virtual private cloud (VPC), providing users with web-based access to CRO resources. CRO is a Structured Query Language (SQL)-based system that renders documents for review, imaging and production. Each SQL database is comprised of 1) already extracted document text and metadata received from parties and/or 2) document text and metadata extracted from original native files received from parties in the case or investigation through the CRO processing tool. In addition, CRO uses search indexes, structured analytics, conceptual analytics tools, and assisted review components to enhance document review effectiveness.

The Civil Division's litigation and investigation functions include affirmative and defensive civil litigation, as well as criminal investigations and prosecutions under consumer protection statutes. All information collected, maintained, used, or disseminated by CRO is used to support the Department's litigation and investigative matters.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

Work performed within CRO may be used by investigative, litigation, and FOIA teams from inception through disposition of the cases and matters. CRO maintains extracted text and metadata received from parties directly, as well as text and metadata extracted from original files provided by parties and processed through the CRO processing engine. Files by parties are processed in connection with the investigative, litigation, or FOIA matters worked on by the Civil Division teams. Data involving those matters may be extremely expansive and diverse, including but not limited to items such as agency files, social media, and other information from computers, cellular devices and other information technologies.

The case team members authorized to use CRO include but are not limited to Civil Division attorneys, legal staff, contractors, and third-party expert witnesses. Attorneys and legal staff analyze documents received from other parties, review for responsiveness any documents that may be produced during case discovery, court order, and FOIA, and may identify and use documents as exhibits for any grand juries, deposition, court motions, or trials. Contractors manage the organization of case data within the CRO workspace. This includes loading documents for review, processing of native file documents for text extraction, and exporting of documents for productions or exhibits. As case experts on the CRO environment, they work with the legal teams to see if any available tools such as but not limited to email threading, textual near duplicate identification, and conceptual analytics indexes that may be used to aid legal teams in their review and analysis.

Third party consultants and expert witnesses may be added to CRO workspaces to assist the legal team with a better understanding of a particular area and/or serve as an expert in a case to generate an expert report and testify at court. By providing such third parties with access to the CRO environment, copies of documents for review do not need to be transmitted in hard copy, email or file transfer. This allows these third parties to review documents in a secured environment with multi-factor authentication obtained through DOJ Login and auditing to guard against any breaches.

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	5 U.S.C. § 301– Departmental housekeeping statute. 5 U.S.C. § 552 – Freedom of Information Act (FOIA). 5 U.S.C. § 552a – Privacy Act of 1974 28 U.S.C. §§ 514–519 – Litigation authority of the Attorney General and the Department of Justice.
Executive Order	

Federal regulation	28 C.F.R. §§ 0.45–0.49 – Civil Division responsibilities and authority.
Agreement, memorandum of understanding, or other documented arrangement	N/A
Other (summarize and provide copy of relevant portion)	

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.

(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 - NonUSPERs	(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, and D	Names of government personnel and members of the public, as they relate to litigation and FOIA/PA matters. Names of government personnel for system administration and audit purposes.
Date of birth or age	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Place of birth	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

Sex	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Race, ethnicity, or citizenship	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Religion	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

(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 - NonUSPERs	(4) Comments
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Tax Identification Number (TIN)	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Driver's license	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Alien registration number	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Passport number	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Mother's maiden name	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Vehicle identifiers	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

Personal mailing address	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Personal e-mail address	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Personal phone number	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Medical records number	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Medical notes or other medical or health information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

(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 - NonUSPERs	(4) Comments
Financial account information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Applicant information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Education records	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Military status or other information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Employment status, history, or similar information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

Certificates	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Legal documents	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Device identifiers, e.g., mobile devices	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Web uniform resource locator(s)	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Foreign activities	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

(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 - NonUSPERs**	**(4) Comments**
Juvenile criminal records information	X	C and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Grand jury information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
Procurement/contracting records	X	B, C, and D	Procurement/contracting records may be a part of necessary litigation documentation and case data such as investigation evidence.
Proprietary or business information	X	B, C, and D	Procurement/contracting records may be a part of necessary litigation documentation and case data such as investigation evidence.
Location information, including continuous or intermittent location tracking capabilities	X	B, C, and D	Procurement/contracting records may be a part of necessary litigation documentation and case data such as investigation evidence.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Video containing biometric data**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Fingerprints**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Palm prints**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

(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 - NonUSPERs**	**(4) Comments**
- **Iris image**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Dental profile**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.

- **Voice recording/signatures**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Scars, marks, tattoos**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **DNA profiles**	X	A, B, C, and D	Any or all items within this category may reside within CRO when relevant to or included in litigation or FOIA/PA records.
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B	Authorized user information is collected for system administration and audit purposes. This includes information collected from outside experts who are considered DOJ contractors. This type of information is collected in response to any activity the expert may have done within the CRO system.
- **User passwords/codes**	X	A, B	Authorized user information is collected for system administration and audit purposes
- **IP address**	X	A, B	Authorized user information is collected for system administration and audit purposes
- **Date/time of access**	X	A, B	Authorized user information is collected for system administration and audit purposes
- **Queries run**	X	A, B	Search and coding history.
- **Contents of files**			Audit logs do not contain contents of files.
(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 - NonUSPERs**	**(4) Comments**

Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Because of the varied nature of the records relevant to litigation or FOIA/PA activities, other types of PII not listed above may be collected, maintained, or disseminated. While it is unlikely that many of the PII types in the rows above would be collected for DOJ employees or other federal employees in their official capacities, employees could potentially be parties to litigation or the subject of investigation.

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone		Email	X		
Other (specify): Data within CRO is typically obtained through the litigation process such as discovery. Such data is typically submitted through counsel or through other forms of legal process. Information may come directly from an individual during the discovery phase through a request for production or via a subpoena and/or in the form of witness statements. Additionally, there is a workspace that contains VCF witness statements. These statements reside within the workspace as both a repository and medium for document review.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Data obtained from foreign government sources would be on a case-by-case basis, governed by separate agreements as applicable.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					

Other (specify): Data within CRO is typically added through the litigation process such discovery. Such data would be submitted through counsel or through an authorized legal process (e.g., subpoena, Request for Production, etc.). Additionally, there is a workspace that contains VCF witness statements. These statements reside within the workspace as both a repository and medium for document review.

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			
	Caseby-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	X	X	X	Data relevant to each matter is placed into specific workspaces and accessed only by personnel who need the data to perform their job function. In addition, data within workspaces may further be secured to specific individuals within the workspace if only those individuals are permitted to see the data.

Recipient	How information will be shared			
	Caseby-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.**

DOJ Components	X	X	X	Data relevant to each matter is placed into specific workspaces and accessed only by personnel who need the data to perform their job function. In addition, data within workspaces may further be secured to specific individuals within the workspace if only those individuals are permitted to see the data. Access to CRO may be provided to individuals in other DOJ components. Case teams may also request a secure data export.
Federal entities	X	X	X	Data relevant to each matter is placed into specific workspaces and accessed only by personnel who need the data to perform their job function. In addition, data within workspaces may further be secured to specific individuals within the workspace if only those individuals are permitted to see the data. Access to CRO may be provided to individuals in other federal agencies. Case teams may also request a secure data export.

Recipient	**How information will be shared**			
	Caseby-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.**

State, local, tribal gov't entities	X	X	X	Data relevant to each matter is placed into specific workspaces and accessed only by personnel who need the data to perform their job function, which, in this context, would include other governmental entities coordinating with the Division. In addition, data within workspaces may further be secured to specific individuals within the workspace if only those individuals are permitted to see the data. Access to CRO may be provided to individuals in state, local, and tribal entities. Case teams may also request a secure data export.
Public				N/A CRO does not share data with the public.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X		X	While rare, adverse or opposing counsel and opposing parties may be given access to specific documents within a database that would otherwise be produced during the discovery process.
Private sector	X		X	Contractors to the Department, who will similarly only have access to data necessary to perform their job function, in supporting the Department's work.
Foreign governments				N/A – CRO does not share data with foreign governments.
Foreign entities				N/A – CRO does not share data with foreign entities.
Recipient	**How information will be shared**			

	Caseby-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.
Other (specify): Expert witnesses	X		X	Data relevant to each matter is placed into specific workspaces and accessed only by personnel who need the data to perform their job function. In addition, data within workspaces may further be secured to specific individuals within the workspace if only those individuals are permitted to see the data.

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.

The data will not be released to the public for this purpose.

Section 5: Notice, Consent, Access, and Amendment

5.1 What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.

Generalized notice is provided via the System of Record Notice (SORN). Depending on the type of case involved, the following SORNs may apply:

- 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);
- DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 Fed. Reg. 26580 (May 4, 2012), and amended at 82 Fed. Reg. (May 25, 2017);
- CIV-001, Civil Division Case File System, 63 Fed. Reg. 8659-8665 (Feb. 20, 1998), as amended at 82 Fed. Reg. 24147 (May 25, 2017).

- CIV-002, Civil Division Case File System: Customs Litigation, last published in full at: 45 Fed. Reg. 2215, 217 (Jan. 10, 1980).

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.

The investigation or discovery process typically does not provide the type of voluntary participation contemplated by this question. Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal process. Collection of information from social media and/or from a webpage is done on a case-by-case basis. In such instances, notice is not provided to individuals as the information is in the public domain.

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.

Individuals and their representatives can request access to information under the Freedom of Information Act or the Privacy Act by submitting requests to the Civil Division (see https://www.justice.gov/civil/foia for submission information). An individual can submit a Privacy Act Amendment or Correction request of their first-party information (see https://www.justice.gov/opcl/doj-privacy-act-requests for submission information). Note, however, that much of the information in CRO may be subject to Exemption 5 of the FOIA (5 U.S.C. 552(b)(5), protecting deliberative process, work-product and other litigation privileges), as well as to Section 552a(d)(5) of the Privacy Act, 5 U.S.C. 552a(d)(5) (excluding from access rights under the Privacy Act information compiled in reasonable anticipation of a civil action or proceeding).

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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** expected completion date 9/30/2025

	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:
	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	**This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** CRO is categorized as a moderate system based on a review of the aggregate impact for confidentiality, integrity, and availability.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Testing of the system is performed before an "Authority to Operate" is issued and during operation by various IT security tools available within DOJ. Monitoring is performed in realtime by Relativity, Civil IT contractors, and Civil IT staff in conjunction with Justice Management Division. Specifically, PII filters are in place so that certain sensitive data, such as Social Security numbers, cannot be transmitted by email to outside parties without Department-required encryption or other security measures. Evaluation is performed in realtime via FedRamp certified system.

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:** CRO complies with DOJ IT Security Standards via PIV card access and DOJ approved multi-factor authentication methods via DOJ Login. Auditing and system logs are stored and maintained in accordance with DOJ policy, as outlined in CRO System Security Privacy Plan.
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**. All contractors granted access to CRO are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role. Contractors are also required to take the Cyber Security Awareness Training (CSAT) annually.
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:**
	Additional training in this system is available to both internal personnel and expert witnesses. The training explains their role-based access to the system and the appropriate permissions to promote information security.

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 CRO users must sign the DOJ Rules of Behavior prior to being granted access to the platform and annually thereafter as required during the lifecycle of the case.

CRO has distinct role-based user profiles created to provide only the necessary permissions to perform their job. System Administrators have access to all workspaces and the environment to troubleshoot, perform maintenance and upgrades to the environment. Content managers are limited in the workspaces they have access to; however, within those workspaces, they can create folders, organize data, and run various analytical tools like email threading. Members of case teams only have access to a specific case and are only given permission to review, analyze, code and search data.

Finally, external users like third party experts are limited to reviewing and analyzing data relevant to their role. They are not permitted to edit, modify, delete or export any

litigation data within the system. Prior to being granted access to CRO, each external user must undergo a security screening by the OLS Security Office in addition to signing the DOJ ROB and attesting to reviewing the CSAT documentation.

All user accounts are subject to automatic logout of a session for 15 minutes inactivity and disabling of their account after 90 consecutive days of inactivity. All user accounts and permissions are reviewed annually to ensure proactive data governance and user account management.

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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

At the conclusion of litigation or following the closure of a FOIA/PA request, the case workspace shall be reviewed for records purposes. If the Division identifies any records that are required to be retained, the relevant data will be exported from CRO and placed within CIV storage, such as AWS Glacier. When in storage, the case data will be kept as a part of the official litigation or FOIA/PA case file and will be maintained under the applicable records schedule. Upon successful export and transport CIV storage, the CRO workspace will be deleted.

Files managed on CRO may include both federal records and non-records that are associated with a variety of different types of Civil Division litigation case files. The retention policies for the files depend on the federal record status as well as the classification of the type of case file to which the files pertain. The Department of Justice record retention schedules are published at https://www.archives.gov/recordsmgmt/rcs/schedules/index.html?dir=/departments/department-of-justice. Record retentions for case files range from approximately 5 years to 65 years after the case closure date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration. Non-records are destroyed when no longer needed for convenience of reference.

CRO will house a workspace containing witness statements provided for VCF claim files. These statements reside within the workspace as a repository for witness statements and a medium for review. These records will be retained in accordance with NARA records schedules and any applicable laws.

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. __X__ 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:

CRO is a tool used for the review and analysis of civil discovery, potential FOIA/PA material, and as a review and repository tool for VCF witness statements related to claims. CRO itself does not constitute a system of records under the Privacy Act. During the civil discovery process, as well as FOIA/PA collection, data may include both Privacy Act records and non-Privacy Act PII from several systems of record and other information systems. The SORNs that apply to the Privacy Act records in CRO include, but are not limited to:

- DOJ-002, Department Computer Systems Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj002_sorn_update.pdf.
- DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 Fed. Reg. 26580 (May 4, 2012), available at: https://www.gpo.gov/fdsys/pkg/FR-2012-05-04/pdf/2012-10740.pdf.
- CIV-001, Civil Division Case File System, last published in full at: 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), available at: https://www.gpo.gov/fdsys/pkg/FR-1998-0220/pdf/98-4206.pdf.
- CIV-002, Civil Division Case File System: Customs Litigation, last published in full at: 45 Fed. Reg. 2215, 217 (Jan. 10, 1980), available at: https://www.justice.gov/opcl/docs/45fr2217.pdf.

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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

CRO processes sensitive litigation, VCF witness statements, and FOIA/PA-related data, including Personally Identifiable Information (PII) and other protected content, which introduces various privacy risks, such as unauthorized access, over-collection, inaccurate data, and unauthorized dissemination. To address these risks, the Civil Division has implemented layered technical, administrative, and physical controls aligned with DOJ, FedRAMP, and NIST requirements.

I. Risks Related to Information Collection

CRO faces privacy risks related to information collection including the over-collection of information and the collection of inaccurate data. CIV has implemented the following measures to mitigate these risks:

- Data Minimization: CRO workspaces are populated only with case-relevant data. Non-relevant PII or sensitive information is excluded wherever possible.
- Encryption: All data is encrypted in transit (TLS 1.2 or higher) and at rest (AES256) per FedRAMP requirements. Sensitive data such as Social Security numbers cannot be emailed outside DOJ without encryption or approved safeguards.
- Retention & Disposal: Upon case closure, required records are exported to approved Civil Division storage (e.g., AWS Glacier) and retained under applicable NARA schedules. The CRO workspace is then securely deleted.

II. Risks Related to Use of Information

CRO faces privacy risks related to the use of information including unauthorized access to the information as well as risks related to the use of Artificial Intelligence (AI)/Machine Learning (ML). CIV has implemented the following measures to mitigate these risks:

- Access Controls: Strict role-based access control (RBAC) ensures users only have the minimum permissions necessary for their assigned tasks. All users must authenticate via DOJ Login multi-factor authentication (MFA). Accounts are reviewed annually and disabled after 90 consecutive days of inactivity.
- Auditing & Monitoring: Comprehensive audit logs capture user actions, including searches, document views, and exports. Logs are reviewed weekly by Civil IT Security staff (Information System Security Officer (ISSO) and Technical POCs), and alerts are monitored in real-time.
- AI/ML Applicability: CRO does have artificial intelligence or machine learning capabilities that can be used in decision-making. Relativity aiR, Transcription, and Translations are automated tools that can be used for an additional fee through the application. At this time, these capabilities are new and must be properly vetted along with strong privacy protections before it can be used widely.

Vetting of the AI/ML capabilities shall include but is not limited to testing of output for inaccuracies, continuous monitoring, training, and secondary review by case teams.

III. Risks Related to Dissemination of Information

CRO faces privacy risks related to the dissemination of information including unauthorized dissemination of the information. CIV has implemented the following measures to mitigate these risks:

- External User Safeguards: Third-party experts undergo DOJ security screening by the Office of Litigation Support (OLS) Security Office, complete CSAT, and are granted read-only permissions limited to assigned case data.
- POA&M Tracking: All identified security or privacy weaknesses are documented in a Plan of Action and Milestones (POA&M) per DOJ. NIST and FedRAMP requirements. POA&Ms are assigned to responsible parties, tracked in the JCAM system, and updated until remediation is complete.