US Department of Justice - Civil Division

Privacy Impact Assessment
for the
Civil Online Relativity Application (CORA)

Issued by:
Allison C. Stanton

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [September 27, 2018]

EXECUTIVE SUMMARY

The Civil Online Relativity Application (CORA) is a collection of three systems (with one child subsystem per platform) maintained by three separate contractors for the Civil Division. CORA is used to effectively store, process, transmit and maintain critical information for the Division related to its litigation and investigation functions. The Civil Division's litigation and investigation functions including affirmative and defensive civil litigation, as well as criminal investigations and prosecutions under particular consumer protections statutes. The system is used as an online web-based repository and application-hosting environment. All information collected, maintained, used, or disseminated by the system is used to support the Department's litigation and investigations. All access to the system is tightly controlled by CORA contract stipulations, Department of Justice security standards, and other statutory security requirements. Once these requirements are met, access may be granted to individuals with a need to review the documents involved in a particular matter; those involved with a particular matter may include Civil Division employees and contractors, agency counsel and investigators, expert witnesses, and opposing counsel. If access to the system has been granted, a user may retrieve information via random, user-generated queries to the system or use the systems analytical tools to find like terms or concepts in the database. Information is transmitted to and from the system via industry-standard HTTPS encryption protocols. None of the three systems have interconnections with any other systems.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

a) The purpose that the records and/or system are designed to serve:
The purpose of the Civil Online Relativity Application (CORA) is to provide an automated litigation support tool, which allows the Division's litigation staff and contractors to: collect and preserve; process, review, and analyze; and produce and

finally present electronic discovery material in connection with the Department's investigative and litigation functions.

b) The way the system operates to achieve the purpose(s):
The CORA system achieves its purpose by making use of several specialty computer programs which collect, index, and present documents for attorneys and staff to review as part of an investigation and/or litigation team. The system at its core contains an indexed SQL database which maintains "meta" information about a specific case and the documents being reviewed for that case. It also makes use of web servers for data presentation and distribution, full text document search servers and indexers, concept cluster and analysis servers and indexers, as well as imaging servers and processors. All of these tools combine in a web browser interface to give litigation professionals a single cohesive tool in which to perform document review and preparation.

c) The type of information collected, maintained, used, or disseminated by the system:
CORA maintains information collected in the course of Civil Division's investigations and litigation. The information may be collected as part of a client-agency's investigation and provided to the Division or may be produced to the Division by an opposing party in the course of the discovery process overseen by the federal courts. This material could include any and all of the following: federal records, participant and custodian's email, word processor documents, spread sheets, scientific findings, research reports and memoranda, depositions, transcripts of discussion and recording, audio files, video files, image files, multimedia presentations, PowerPoint presentations, personal notes, letters and correspondence. Publicly available information may also be incorporated if deemed relevant to the litigation. Publicly available information may include, but is not limited to, newspaper articles and other published journalism, public records, court records, social media information, and other data traditionally considered "open source." This material is used in the document discovery process of litigation and is only disclosed and distributed as prescribed and overseen by the court.

d) Who has access to information in the system:
The information maintained in CORA may be accessed by authorized Civil Division employees, other federal employees and contractors. Only those persons and parties who have a demonstrated need to have access to the collected information are given access to the system. Once a user has been granted access to the material, the user is limited to only that information necessary to perform his or her particular work function. Before access is authorized, the individual's access rights and purpose for accessing the documents is reviewed by the Civil Division's IT security staff and the investigation and/or litigation team.

e) How information in the system is retrieved by the user:
Within the information set a user can access, the user can: retrieve information by performing full text searches and browse information which may be organized by document number, identifier, creator or custodian, or legal matter. Information within

the system can also be grouped into user-defined folders for retrieval based on document meta-data such as: date, source, subject, type of material, file format, concepts, or user-defined tags.

f) How information is transmitted to and from the system:
The system allows for the ingestion (loading) and dissemination (productions and exports) of material – both processed and unprocessed. Unprocessed material is raw data from the source that provides the Civil Division information – another agency, a seized hard drive, etc. Processed means that the Civil Division ingested the data and created it, to a certain extent. The mechanism for this transmission is to place the electronic documents on the Civil Division's Office of Litigation Support (OLS) servers network disk storage and to instruct the system (through supplied applications) to ingest the documents into a specific (segregated) area for the particular case. The ability to add material to the system is a specific controlled and limited user role. For the dissemination of material the process is reversed. The system can be instructed (through supplied applications) to export out material for review to a specific (segregated) area for the particular case. The ability to export material from the system is a controlled and limited user role.

g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):
The CORA system interconnects with Office of Litigation Support Servers Systems (OLSSS) and Civil Division's Justice Consolidated Office Network (CIV-JCON), which is a document repository tool customized to the Civil Division's specifications.

h) Whether it is a general support system, major application, or other type of system:
The CORA system is a minor application.]

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card	X		
Other identifying numbers (specify): [ ]					

General personal data					
Name	X	Date of birth	X	Religion	X
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	X
Other general personal data (specify):					

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	X
Work address	X	Business associates	X		
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system/audit data (specify):					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	X
Telephone		Email	X		
Other (specify): Documents are obtained through discovery, the processes by which parties to a lawsuit, hearing, or other legal proceeding are required to exchange documents relevant to the case at hand.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please 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. Please describe the choices that the component 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 described above, the information contained and managed on CORA is provided to the Civil Division in the course of litigation or an investigation. Data is collected pursuant to the rules of overseeing federal court litigation. The documents are typically provided by another federal or state entity involved in the investigation or by the opposing party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with collecting records from other entities is that they will share information outside the scope of the investigation or not properly identify the data being ingested into the system as containing personally identifying information. Preventing the exposure of the data once it is received by the Civil Division minimizes the risk that personal information will be shared outside the team of individuals working on a particular matter. To this end, the Civil Division places strict access controls on CORA via physical and electronic means in order to secure the information.

The potential compromise of PII in the system is also a risk. To address that concern, the Civil Division places strict access controls on CORA via physical and electronic means in order to secure the information. For example, Civil Division employees and contractors are only granted access to databases on the system that support a matter they are working on. If an employee or contractor leaves or is reassigned, the account access is disabled or access to a particular database may be rescinded. If significant PII is collected incidentally during litigation discovery and production, access to those particular data collections may be further restricted to selected individuals among the case litigation team.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
X	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	[ ]	To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	[ ]	For administering human resources programs
X	For litigation		
[ ]	Other (specify): [ ]		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

[The Civil Division's litigation mission includes civil and criminal enforcement investigations and actions as well as defensive work on behalf of the United States government. The information collected is used to accomplish activities inherent in the Division's investigations and litigation, including reviewing documents for relevance and privilege claims, tracking use of documentary evidence in litigation, preparing witness kits/binders for depositions and hearings, determining and organizing the facts about the case, and selecting exhibits for trial. Collection, maintenance, and use of the information supports the Civil Division's litigation and administrative functions.]

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	[28 U.S.C. §§ 514-19]
[ ]	Executive Order	[ ]
X	Federal Regulation	[28 C.F.R. §§ 0.45-0.49 Subpart I]
[ ]	Memorandum of Understanding/agreement	[ ]

[ ]	Other (summarize and provide copy of relevant portion)	[ ]

3.4 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.)

[Data will be retained in the system until the DOJ Civil Division case attorney and the Office of Litigation Support determine that the litigation materials no longer need to be stored on the system, typically after a case has closed or settled and the information is not needed for other cases or investigations. In consultation with the attorney assigned to the matter, the Office of Litigation Support will dispose of records that do not need to be maintained in any form pursuant to the Division's obligations under the Federal Records Act, as explained below. Records that must be maintained will be retained in accordance with the applicable retention schedule. When closing or settling a case and removing it from the system, the data is saved to an external hard drive or other media and provided to the attorney closing the case. The data is then deleted from CORA. The space previously used by the closed case is re-used and made available for other matters. A copy of the data will remain on CORA's backup tapes for approximately one year after the case closes and the backup tape is overwritten with new data. Data will be disposed of after consultation with the case attorney. Archiving a case leaves the data with the attorney and the space previously used by the case is re-used (deleted, then made available elsewhere).

Files managed on CORA 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/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060. 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.]

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component 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 a potential risk to privacy that could result from the improper access to information in the system; however, security protections that authorize and limit a users' access to information within the system mitigate the risk. Physical controls such as secured entrances and security officers protect access to the building where the servers and workstations are

located. To access the system, the Civil Division enforces Department standards for accessing a network system, such as Personal Identity Verification (PIV) card entry. In addition, before a user is granted access to a system hosted on CORA, the user completes required security training, including cybersecurity training and privacy training targeted to the user's role. Individuals outside the Civil Division are required to sign a confidentiality agreement and rules of behavior documents before they are provided with access to accounts. In addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

Access to the system is granted on a need-to-know basis. For example, Civil Division attorneys, other staff members, other federal employees, and contractors are only granted limited access to the matters they work on, not the entire system.

There are monitoring and auditing tools for each system to review user activity, so the Civil Division can monitor user access within the system. Access controls are backed up by detailed audit logs that provide a detailed overview of how data has been accessed and used within the system to ensure compliance with applicable handling policies. In addition, the system generates detailed metadata and audit logging information that can help administrators manage data retention schedules as established for the system. Data can be identified based on its age, the specific case that it is supporting, whether the data remains in active use, and other parameters that might be relevant to a data retention decision. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system.

In addition to these protections, all disk volumes and backup tapes containing PII are encrypted via hardware-based FIPS 140-2 encryption mechanisms. In addition, CORA employs intrusion detection and prevention systems to detect and prevent potential malicious activity, changes to the network, and traffic anomalies. Further, CORA backs up data regularly and controls access to data stored on the application. Frequent network and system vulnerability scanning ensure all vulnerabilities and associated risks are addressed and mitigated in a timely manner. A combination of access, logical, and technical controls provides a robust suite of policies, procedures, and technology that ensure PII and other Sensitive But Unclassified (SBU) are protected at all points in the CORA system.]

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X		X	

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public				
Private sector	X		X	Contractors to the Department
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Disclosure or sharing of information maintained in CORA occurs when information is produced in discovery or when individuals outside the Civil Division are granted direct access to a particular set of information maintained in the system. For individuals that have direct access to the system, access restrictions described in Section 3.5 apply to the system. Information access in the system is granted on a need-to-know basis. Users both inside and outside the Civil Division are only granted limited access to the matters they work on, not the entire system. Users outside the Civil Division may include investigators from another component or agency, partners at the United States Attorney's Office, or expert witnesses. There are monitoring and auditing tools for each system to review user activity, so the Civil Division can monitor user access within the system. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system. The process for establishing and reviewing accounts includes application and monitoring of initial distribution of accounts. Credentials are controlled according to DOJ and NIST standards. The controls include password management, including password composition, history, compromise, and changes. The processes also include monitoring account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of need-to-know requirements. Additionally, the processes include monitoring of access privileges monthly, to further enforce need-to-know requirements. When a user account is created, the account is provided the least possible privileges for the user to perform tasks related to the investigation and litigation activities. CORA logs and tracks unsuccessful logins and automatically locks the account when the maximum number of consecutive unsuccessful attempts are exceeded. A system administrator must be called to unlock the account. The system also forces re-authentication after the specified period of inactivity. For users who access CORA

outside of a DOJ facility, remote access via Virtual Private Network is controlled and monitored. Encryption is used to protect the confidentiality of remote access sessions and secure remote access tokens are implemented to authorize and control access. Remote users are presented with Department policies regarding authorized use before login each time they are required to authenticate or re-authenticate.

Audit trails are generated by CORA. The audit trails detect intrusion and are used to identify data misuse. CORA also is configured to protect audit information and tools from unauthorized access, modification and deletion. The intrusion detection audit trails are reviewed on a weekly basis, or when an incident is suspected. The application audit trails are reviewed on an as-needed basis. In addition, CORA employs an intrusion detection system to detect vulnerabilities, changes to the network and traffic anomalies. Further, CORA backs up data regularly and controls access to data stored on the Application.]

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information 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 7.	
[ ]	Yes, notice is provided by other means.	Specify how: [ ]
[X]	No, notice is not provided.	Specify why not: [Documents are obtained through court order, warrant, subpoena, discovery requests, and other such methods. Individuals do not directly provide information to this system; rather, information about individuals may be contained in documents collected from opposing parties and client agencies in the course of litigation. For social media captures and web site collections, notice is not provided to individuals as the information collected is in the public domain.]

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

[ ]	Yes, individuals have the opportunity to decline to provide information.	Specify how: [ ]
[X]	No, individuals do not have the opportunity to decline to provide information.	Specify why not: [Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may challenge the relevance of the information and not produce

		the information in litigation, but that challenge would be determined before the information is collected and maintained by CORA. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.]

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

[ ]	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: [ ]
[X]	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: [Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by CORA. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.]

5.3 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

[Unless individuals are opposing parties in litigation, individuals do not provide information directly to the Civil Division for use in CORA. Individuals who are opposing parties in litigation can object to the Division obtaining the information through the discovery process. Individuals whose information is collected in the course of litigation involving another entity, such as another government agency or business entity, may have the opportunity to consent at the collection from the other entity. If another government agency is involved in the investigation or litigation, the agency's System of Records Notice would provide notice that the information may be shared with the Department of Justice for the context of a civil or criminal investigation or litigation. For information collected from the internet, notice is not provided to individuals as the

information collected is in the public domain.]

Section 6: Information Security

6.1 Indicate all that apply.

[X]	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: [2/15/18] If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: [ ]	
[X]	A security risk assessment has been conducted.	
[X]	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: [The Civil Division has applied the policies and procedures outlined in the DOJ Security Authorization Handbook and in DOJ's security tracking tool, Cyber Security and Assessment Management application.]	
[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 real-time by not only Civil IT staff but also 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 real-time via several packages of software, in place on local machines and scanning network transmissions.]	
[X]	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: [CORA system complies with DOJ IT Security Standards via PIV card access, attribution to named individuals, disallowing test or training accounts and strict compartmentalization of information and accounts.]	
[X]	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
[X]	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
[X]	The following training is required for authorized users to access or receive information in the system:	
	[X]	General information security training
	[X]	Training specific to the system for authorized users within the Department.
	[X]	Training specific to the system for authorized users outside of the component.
	[ ]	Other (specify): [ ]

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

[The CORA security plan, including administrative and technological controls, is documented in accordance with DOJ guidance, policies and directives. The CORA system exists

on a physically secure, environmentally protected, DOJ network protected by firewalls, and is administered by both DOJ and non-DOJ contractor personnel. CORA system's connection to the JCON network and the outside world is firewall protected, constantly monitored via intrusion detection software as well as housed within another JCON system (CIV-JCON). Firewall and operating system security are tested monthly. Patches are applied as appropriate to maintain system security. System access is monitored by inspection of event logs, system logs, web logs, database application logs, and firewall logs.

Access to CORA is granted only to DOJ-approved individuals who have signed a confidentiality agreement and system rules of behavior. Access to specific databases/folders/material is granted on a need-to-know basis by user account and password. All CORA accounts are "named user" accounts assigned to a single individual and require PIV authentication. A documented process exists for requesting, granting, and reviewing account activity, and terminating accounts. Test, training, or temporary accounts are not permitted in order to accurately log the individual accessing the information.]

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

[X]	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: [JUSTICE/CIV-001 *Civil Division Case File System*, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf.]
[ ]	Yes, and a system of records notice is in development.
[ ]	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

[Information specifically pertaining to US citizens and/or lawfully admitted permanent resident aliens can be retrieved from the system, but is handled in strict accordance with all federal regulations regarding PII. CORA offers a variety of retrieval solutions, which generally allow a full-text or fielded search on document data and metadata collected (e.g. date sent, from, to, cc as collected or produced via the discovery protocols). A full-text search uses the database's index to quickly sift through every word (of every record) that can be entered in the database. The user can search and retrieve a list of documents and then view the documents found by the search. CORA privacy protections do not differ depending on whether the information about an individual is a U.S. citizen or a lawfully admitted permanent resident alien.]