United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
[DOJ RelativityOne]

Issued by:
[Arthur E. Gary
JMD Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [June 2, 2021]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The RelativityOne Software-as-a-Service (SaaS) e-Discovery cloud tool enables U.S. Department of Justice (DOJ or "the Department") litigation components to ingest, search, analyze, and produce large amounts of data that may be relevant to support DOJ litigation, discovery, or disclosure of document requests, as mandated by law and DOJ policy. RelativityOne uses many of its core capabilities to accomplish DOJ discovery and litigation functions, such as data transfer, data ingestion and structuring, search and machine learning for active learning to continuously assess what is important to users and serve up relevant information faster,[1] document review and coding, and product and export. RelativityOne is currently hosted within the Microsoft Azure Government cloud.[2] This system will be offered as an enterprise offering within the DOJ IT Services Catalog for litigation components to leverage in their organization's environment as appropriate to fulfill the Department's mission.

JMD prepared this Privacy Impact Assessment because RelativityOne will collect, use, and maintain personally identifiable information (PII). Due to the nature of e-discovery data collection and processing, various types of PII will potentially be a part of gathered evidence in support of legal investigations. Such PII will include DOJ end-users contact information, and non-DOJ individuals who communicate with DOJ end-users.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, 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.

DOJ is responsible for, among other tasks, enforcing the law, defending the interests of the United States according to the law, seeking just punishment for those guilty of unlawful behavior, and ensuring fair and impartial administration of justice for all Americans. As part of these responsibilities, DOJ has a number of litigating components that are responsible for representing the United States Government in most domestic and foreign court, grand jury, administrative, or adjudicative bodies. DOJ litigating components must ingest, search, analyze, and produce large amounts of data relevant to support DOJ litigation, discovery, or disclosure of document requests, as mandated by law and DOJ policy.

---

[1] "Machine learning" is a subset of artificial intelligence that "involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets." Cong. Research Service, Artificial Intelligence and National Security (Nov. 21, 2019) https://fas.org/sgp/crs/natsec/R45178.pdf. RelativityOne leverages a "active learning workflow" to assist users better assess the relevancy of e-discovery documents, actively displaying more relevant data to users based on their actions. JMD will ensure that any use of machine learning within RelativityOne will be conducted in accordance with Executive Order No. 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, 85 Fed. Reg, 78939 (Dec. 8, 2020).

[2] Azure Government delivers a dedicated cloud infrastructure enabling government agencies and their partners to transform mission-critical workloads to the cloud. Azure Government services handle data that is subject to certain government regulations and requirements. More information can be found at: https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-welcome.

RelativityOne is a cloud-based tool providing litigation components with one secure and extensible platform to perform e-discovery and other litigation processes. RelativityOne assists attorneys, paralegals, and other DOJ staff in reviewing investigation, litigation, and disclosure records about a specific case and the documents being reviewed for that case, handle legal holds[3], and provide a central workspace to bring case strategy and e-discovery together.

For investigations, RelativityOne provides the capability to search/query all relevant documentation related to an investigation and allow for quicker analysis and also visualize these documents through customized "dashboards."

For legal holds, RelativityOne has an integrated solution for complete, customized legal holds automated management which will assist components in identifying, preserving, and tracking relevant data when litigation is anticipated. RelativityOne also includes templates so hold notices would not need to be written from scratch.

For case strategy, RelativityOne features allow end users to craft their own narrative and understanding of the documents by simultaneously linking artifacts together, review videos, transcripts, other documents, automate timelines, and collaborate with case stakeholders.[4]

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
x	Statute	5 U.S.C. § 301 (agency operations) 28 U.S.C. § 516 (conduct of litigation) 28 U.S.C. § 534 (acquisition, preservation, and exchange of identification records and information; appointment of officials) 28 U.S.C. § 547 (duties of United States Attorneys)
	Executive Order	
x	Federal Regulation	28 C.F.R. Chapter 1
	Agreement, memorandum of understanding, or other documented arrangement	
x	Other (summarize and provide copy of relevant portion)	Federal Rules of Criminal Procedure Federal Rules of Civil Procedure Federal Rules of Evidence Federal Rules of Appellate Procedure Justice Manual

[3] A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. https://www.exterro.com/basics-of-e-discovery/legal-hold

[4] A detailed review of RelativityOne's functionality can be found on the RelativityOne User Guide: https://help.relativity.com/PDFDownloads/R1_PDF/RelativityOne%20-%20User%20Guide.pdf.

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 - Non-USPERs	(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, D	All information categories may apply to this system, as any of the PII of the people identified in column #3 can potentially be collected as part of litigation and the e-discovery process.
Date of birth or age	X	A, B, C, D	See comment, above.
Place of birth	X	A, B, C, D	See comment, above.
Gender	X	A, B, C, D	See comment, above.
Race, ethnicity or citizenship	X	A, B, C, D	See comment, above.
Religion	X	A, B, C, D	See comment, above.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	See comment, above.
Tax Identification Number (TIN)	X	A, B, C, D	See comment, above.
Driver's license	X	A, B, C, D	See comment, above.
Alien registration number	X	A, B, C, D	See comment, above.
Passport number	X	A, B, C, D	See comment, above.
Mother's maiden name	X	A, B, C, D	See comment, above.

(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 - Non-USPERs	(4) Comments
Vehicle identifiers	X	A, B, C, D	See comment, above.
Personal mailing address	X	A, B, C, D	See comment, above.
Personal e-mail address	X	A, B, C, D	See comment, above.
Personal phone number	X	A, B, C, D	See comment, above.
Medical records number	X	A, B, C, D	See comment, above.
Medical notes or other medical or health information	X	A, B, C, D	See comment, above.
Financial account information	X	A, B, C, D	See comment, above.
Applicant information	X	A, B, C, D	See comment, above.
Education records	X	A, B, C, D	See comment, above.
Military status or other information	X	A, B, C, D	See comment, above.
Employment status, history, or similar information	X	A, B, C, D	See comment, above.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	See comment, above.
Certificates	X	A, B, C, D	See comment, above.
Legal documents	X	A, B, C, D	See comment, above.
Device identifiers, e.g., mobile devices	X	A, B, C, D	See comment, above.
Web uniform resource locator(s)	X	A, B, C, D	See comment, above.
Foreign activities	X	A, B, C, D	See comment, above.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	See comment, above.
Juvenile criminal records information	X	A, B, C, D	See comment, above.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	See comment, above.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, D	See comment, above.
Grand jury information	X	A, B, C, D	See comment, above.

(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 - Non-USPERs	(4) Comments
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	See comment, above.
Procurement/contracting records	X	A, B, C, D	See comment, above.
Proprietary or business information	X	A, B, C, D	See comment, above.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	See comment, above.
Biometric data:	X	A, B, C, D	See comment, above.
- **Photographs or photographic identifiers**	X	A, B, C, D	See comment, above.
- **Video containing biometric data**	X	A, B, C, D	See comment, above.
- **Fingerprints**	X	A, B, C, D	See comment, above.
- **Palm prints**	X	A, B, C, D	See comment, above.
- **Iris image**	X	A, B, C, D	See comment, above.
- **Dental profile**	X	A, B, C, D	See comment, above.
- **Voice recording/signatures**	X	A, B, C, D	See comment, above.
- **Scars, marks, tattoos**	X	A, B, C, D	See comment, above.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, D	See comment, above.
- **DNA profiles**	X	A, B, C, D	See comment, above.
- **Other (specify)**			See comment, above.
System admin/audit data:	X	A	System maintains system logs and other audit data on system and user activity.
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**	X	A	

(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 - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Given the purpose of RelativityOne, any PII relevant and necessary to Department litigation, investigations, eDiscovery, and disclosure activities could be maintained in this system, including PII not otherwise within the above referenced categories.

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	x	Hard copy: mail/fax	x	Online	x
Phone	x	Email	x		
Other (specify): Documents can be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including directly from the individual about whom the information pertains.					

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): Documents can be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including other government sources.					

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

Other (specify): Documents can be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including non-government sources.

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			
	Case-by-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	JMD will have direct access to RelativityOne to manage/administer component offerings and perform continuous monitoring of system in line with DOJ's cybersecurity requirements. _____
DOJ Components	x	x	x	DOJ litigating components requesting the ability to leverage the system within their organization will maintain direct access to the system. JMD must authorize new users, prior to use.
Federal entities	x			DOJ may share case/e-discovery information and collaborate with other federal entities on a case-by-case basis, as needed.
State, local, tribal gov't entities	x			DOJ may share case/e-discovery information and collaborate with SLT entities on a case-by-case basis as needed.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	x			DOJ may share data pertaining to e-discovery to opposing counsel or need-to-know parties for litigation purposes.
Private sector	x		x	Contractors to the Department
Foreign governments				
Foreign entities				
Other (specify):				

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.

Information processed and stored within DOJ RelativityOne will not be released to the public for "Open Data" purposes or for research or statistical analysis purposes.

Section 5: Notice, Consent, Access, and Amendment

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

Individuals' data are gathered through court order, warrant, subpoena, discovery request, and other such methods. In most cases, information about individuals may be contained in documents collected from various parties in the course of litigation. To the extent individualized notice is required by law, court rules, or DOJ policy, the Department will provide varying degrees of direct notice to individuals whose privacy interests are implicated by these orders/requests. Opposing counsel or the court may also provide individualized notice, depending on the circumstances. The Department, however, is not required to provide individualized notice to everyone whose PII may be implicated.

That said, individuals are provided generalized notice of the Department's maintenance of these records through the Department's published System of Records Notices (SORNs). The applicable SORNs include:

- JUSTICE/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)
- JUSTICE/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)

The records created, compiled, and maintained in this system to accomplish the Department's investigations, litigation, and discovery functions, may also be covered by the Department's litigation and general leadership case file SORNs, including:

- JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017)

- JUSTICE/ATR-001, Antitrust Division Expert Witness File, last published in full at 54 Fed. Reg. 42060, 061 (Oct. 13, 1989), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- JUSTICE/CIV-001, Civil Division Case File System, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- JUSTICE/USM-001, U. S. Marshals Service Badge & Credentials File, last published in full at 72 Fed. Reg. 33515, 516 (June 18, 2007), and amended at 82 Fed. Reg. 24151, 162 (May 25, 2017)

- JUSTICE/USM-013, U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files, last published in full at 72 Fed. Reg. 33515, 529 (June 18, 2007), and amended at 82 Fed. Reg. 24151, 165 (May 25, 2017)

- JUSTICE/OIG-001, Office of the Inspector General Investigative Records, last published in full at 72 Fed. Reg. 36725 (July 5, 2007), and amended at 82 Fed. Reg. 24151, 160 (May 25, 2017)

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.

Given the investigation, litigation, and disclosure equities of the Department, individuals will generally not be provided an opportunity to voluntarily participate in the collection, use, or dissemination of information accessible to RelativityOne.

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 have been notified that the records maintained in RelativityOne can be accessed or amended, in accordance with DOJ regulations, by following the access and amendment procedures in the applicable SORNs, above. Individuals may also follow the procedures outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations. The records maintained in RelativityOne, however, may be subject to certain exemptions to the access and amendment procedures, as articulated in the applicable SORNs, above, and in Subpart E, Part 16, Title 28, Code of Federal Regulations.

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 an ATO has not been completed, but is underway, provide status or expected completion date:** Expected ATO - May 2021 **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:** No current active POAMs
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** RelativityOne FedRAMP package was reviewed by the OCIO Cybersecurity Staff (CSS). The cloud service provider, Relativity, is responsible for securing and enforcing identified security controls and informing the DOJ of any incidents.
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:** Specified audit log events tied to system and user actions are recorded and reviewed on a regular basis within cloud service provider's SIEM tool. The DOJ Justice Security Operations Center (JSOC) also ingests logs.
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**.
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:** Relativity does provide training for users to learn proper functionality of the software and avoid improper use.

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?

RelativityOne has a security categorization of FISMA moderate, and has assessed and implemented all applicable security controls to ensure protections commensurate with the impact to Department from any unauthorized access or disclosure of information. A full security control assessment of the DOJ RelativityOne system has been completed and review

of the FedRAMP package produced by Relativity, who is the software company that developed the RelativityOne software, that goes into depth of the hosting infrastructure and controls implemented by the vendor. The principle of least privilege is enforced through privileged user accounts and non-privileged accounts that will not have administrative rights. Users are also only able to operate the system on a government furnished equipment and while connected to the DOJ network. Users will also be required to log in using multi-factor authentication (PIV and PIN).

All data-at-rest and in-transit is encrypted compliant with the Federal Information Processing Standard (FIPS)140-2[5] validated encryption modules. A periodic review of role-based access audit logs will be done to detect any possibly unauthorized access.

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.)

Data will be retained in the system until 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 and in line with the NARA record retention schedule DAA0060-2017-0007 (Records Documenting Compliance with Preservation Obligations for Component Information) which requires data to be destroyed within 3 years after preservation obligation ends. Data custodians within components will be tasked with reviewing the audit trail to determine when and which data can be destroyed.

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:

Below are the applicable System of Records Notices (SORNs):

- JUSTICE/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)
- JUSTICE/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)

[5] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/publications/detail/fips/140/2/final.

The records created, compiled, and maintained in this system to accomplish the Department's investigations, litigation, and discovery functions, may also be covered by the Department's litigation and general leadership case file SORNs, including:

- JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017)
- JUSTICE/ATR-001, Antitrust Division Expert Witness File, last published in full at 54 Fed. Reg. 42060, 061 (Oct. 13, 1989), and amended at 82 Fed. Reg. 24147 (May 25, 2017)
- JUSTICE/CIV-001, Civil Division Case File System, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), and amended at 82 Fed. Reg. 24147 (May 25, 2017)
- JUSTICE/USM-001, U. S. Marshals Service Badge & Credentials File, last published in full at 72 Fed. Reg. 33515, 516 (June 18, 2007), and amended at 82 Fed. Reg. 24151, 162 (May 25, 2017)
- JUSTICE/USM-013, U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files, last published in full at 72 Fed. Reg. 33515, 529 (June 18, 2007), and amended at 82 Fed. Reg. 24151, 165 (May 25, 2017)
- JUSTICE/OIG-001, Office of the Inspector General Investigative Records, last published in full at 72 Fed. Reg. 36725 (July 5, 2007), and amended at 82 Fed. Reg. 24151, 160 (May 25, 2017)

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?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

As indicated in the table within section 3.1, every information category will potentially be stored within DOJ RelativityOne given the nature of litigation materials and e-discovery. The main potential privacy risks associated with this system and the data that is being stored and processed is: (1) unauthorized access, (2) unauthorized disclosure or breach of PII, and (3) data over-collection.

To mitigate these risks, only cleared DOJ personnel that have a need-to-know, with DOJ network

accounts and email addresses, will have authorized access to this system using two-factor authentication (PIV card and PIN). Litigating components that require use of this system will need to authorize the system internally with their designated risk/authorizing official prior to use within their environment. To enforce need-to-know requirements, Components will then have a separate instance created so they only have access to documents managed by their respective component.

To further mitigate privacy risks resulting from the sensitive information, including PII, maintained in RelativityOne, JMD has implemented numerous security controls, consistent with Section 6, above. For instance, RelativityOne is a Federal Risk and Authorization Management Program (FedRAMP) authorized software solution. The FedRAMP is a standardized security assessment and authorization process for cloud products and services used by the U.S. federal agencies. As a result, RelativityOne was reviewed by an authorized third-party assessment organization, and authorized to operate by the Environmental Protection Agency's authorizing official. The JMD, Office of the Chief Information Officer, Cybersecurity Services Staff, also completed a review of the software solution prior to acquisition. A DOJ authority-to-operate (ATO) will be granted as an assessment and documentation of NIST Special Publication 800-53 security and privacy controls have been implemented.

To further safeguard information maintained in RelativityOne, all data at rest, including backups, are encrypted with Storage Service Encryption, which is deemed to be FIPS 140-2 validated. Data in transit, which is both internal and external web traffic, is encrypted as well using Transport Layer Security (TLS) 1.2.[6] The Information Security System Officer and system stakeholders will meet with the cloud service provider, Relativity, periodically to perform continuous monitoring of security controls and any changes that may occur. Relativity has incident response procedures that include preparation, detection and analysis, containment, eradication, and recovery and also collaboration/notification of DOJ. An annual system contingency plan and incident response tabletop exercise will be performed in accordance with continuous monitoring guidance.

To mitigate the risk of data over-collection, the users that are a part of the litigating components are trained to perform e-discovery in a manner that data collection is intended to identify information relevant to the purpose of the litigation matter at hand.

By Department Order, all DOJ users (federal and contractor) with access to Department networks, must complete annual Cyber Security Assessment Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to

---

[6] The "Transport Layer Security" protocol is used "to secure communications in a wide variety of online transactions . . . . Any network service that handles sensitive or valuable data, whether it is personally identifiable information (PII), financial data, or login information, needs to adequately protect that data." NIST, Special Publication 800-52, rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (Aug. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf.

ensure that DOJ employees and contractors comply with this training.