



PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.

All entries must be Times New Roman, 12pt, and start on the next line.

If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: RelativityOne Government	
Preparer: Charleen M. Townsend	Office: OMS - eDiscovery Division, Office of Enterprise Information Programs.
Date: June 1 st , 2020	Phone: (202) 566-0873 or (202) 740-7936 (cell)
Reason for Submittal: New PIA <u> X </u> Revised PIA <u> </u> Annual Review <u> </u> Rescindment <u> </u>	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input checked="" type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u>	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u>	

Provide a general description/overview and purpose of the system:

The Relativity One (RelativityOne Government) is an electronic tool that exists in the cloud and will assist with the preservation, search, processing, review and production of electronically stored information (ESI) in support of legal discovery or to respond to other formal information requests, such as FOIA requests and congressional inquiries.

The information collected and maintained by RelativityOne Government is not new data, but copies of existing data that reside on EPA systems. The RelativityOne Government tool does not specifically collect PII data elements; however, if PII is collected as part of a discovery matter, then the PII will be maintained in the system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The statutory authority for the RelativityOne Government tool can be found in 44 U.S.C. 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

No, the security plan is currently undergoing creation by Relativity. In the June/August 2020 timeframe we will receive their SAR and begin to review their package. The plan is for the tool to receive an ATO by end of September 2020.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, the data will be maintained and stored in the Relativity Cloud. The provider is currently undergoing FedRamp certification. The CSP will provide SaaS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

- eDiscovery Litigation Hold Files. The litigation hold files contain the names and email addresses of EPA employees and EPA contractors, interns, or grantees who have been provided EPA email addresses and who have been identified as custodians of information that needs to be preserved in the anticipation of litigation.

- eDiscovery Case Tracking Files. The case tracking files contain information about the cases created in response to a litigation, investigation, Freedom of Information Act (FOIA) matter or other formal information request.
- eDiscovery Collection Files. The collection files contain all information responsive to designated search criteria that relate to a litigation, investigation, FOIA matter or other formal information request. Information collected and contained in the system can be wide-ranging and potentially include emails, documents and other sources of ESI collected from custodians and may contain personally identifiable information. The information in the system will also contain the names and EPA email addresses of EPA employees, contractors, and grantees who have been identified as potential information custodians. Privacy information may be included in the ESI collected and maintained in the system.

2.2 What are the sources of the information and how is the information collected for the system?

The sources of information are custodians' local workstations, network file servers, collaboration tools, electronic records repositories, email and loose electronic documents (e.g., MS Word, MS PowerPoint, PDF, etc.). The information is extracted from its native source using the RelativityOne Government Tool, which is operated by EPA's eDiscovery technical team. Collections are based on custodian, date range and search or filtering criteria (e.g. keywords) that relate to the matter.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use information from commercial sources, such as information obtained from data aggregators. The system does not collect publicly available data, meaning information received from the internet, news feeds or from state or local public records, such as court records. Any data that reside in the RelativityOne Government Tool have been collected from other EPA systems to determine the data's relevance to a particular matter, and the collected data may or may not include data that EPA has made or will make available to the public.

2.4 Discuss how accuracy of the data is ensured.

The data retained in the system are copies of information already residing on other EPA systems. Therefore, the accuracy of the data in the RelativityOne Government Tool depends on the accuracy of the data in the source systems. Data is not modified in Relativity as this tool is not meant to store anything other than forensic copies of records to respond to court ordered discovery or other statutorily required requests for EPA documents.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is a risk that in the process to collect and determine whether information is relevant to a matter, more information is collected and maintained in the RelativityOne Government Tool than is relevant to the matter.

Mitigation:

To mitigate this risk, the information that resides in the system that is determined not to be relevant to the matter will not be further disseminated beyond those individuals responsible for determining its relevance to the matter. Further, CIO Procedure 2155-P-03, *Collection and Retention Procedures for Electronically Stored Information (ESI) Collected Using E-Discovery Tools*, describes the data retention process for ESI collected using the RelativityOne Government Tool. The information residing in the RelativityOne Government Tool is necessary for legal discovery and to respond to FOIA requests, congressional inquiries and other formal requests for information. Part of the process includes determining relevance of the information and not all information will be determined relevant for the matter for which it was collected.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Access to the RelativityOne Government Tool is restricted to a limited number of authorized users with the appropriate security clearances and password permissions. Access to the system is further limited by user type. System administrators have full access to the tool suite, including the ability to perform administrative functions. Other users have limited access particularized to the specific functions and data they need to perform in the tool. This access is controlled by a series of permissions within dedicated workspaces/databases for each specific request.. Authorized users include federal and contract staff located throughout the country. The system is maintained in secure areas and buildings with physical access controls.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access controls the Cloud Service Provider, Relativity, has implemented for RelativityOne Government are included in their SSP and approved as part of the Agency ATO and FedRAMP Authorization.

The access controls the eDiscovery Division (EDD) is responsible for are specifically addressed in the system security plan EDD has developed for RelativityOne Government based on the customer response matrix. These controls will be assessed annually.

Will be documented in the CRM.

3.3 Are there other components with assigned roles and responsibilities within the system?

Authorized users of the RelativityOne Government Tool include federal and contract staff located throughout the country in EPA's Program Offices and Regions. This includes eDiscovery technicians, case managers and other federal and contract staff supporting the Discovery Services Program in OEI and other EPA Program Offices and Regions.

Employees reviewing collected data to determine the data's relevance to a particular matter will have access to the information maintained in the RelativityOne Government Tool, as appropriate. These employees may be assigned to the various EPA's Program Offices and Regions.

3.4 Who (*internal and external parties*) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Authorized users of the RelativityOne Government Tool include federal and contract staff located throughout the country. This includes eDiscovery technicians, case managers and other federal and contract staff supporting the Discovery Services Program. Employees reviewing collected data to determine its relevance to a particular matter will have access to the information maintained in the RelativityOne Government Tool, as appropriate.

FAR clauses 52.224-1 and 52.224-2 have been included in the contract for support of the Discovery Services Program and will be included in future contracts.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

EPA Records Schedule 1012

- Close at end of calendar year, or when superseded by a new iteration, or no longer needed for investigative or security purposes, whichever is later; or when system is terminated, defunded, removed from public access, or otherwise does not serve the original purpose.
- Data are destroyed 7 years after file closure.

EPA Records Schedule 0089

- Close when no longer needed for current agency business.
- Destroy immediately after file closure.

Reason for retention:

- **eDiscovery Litigation Hold Files.**

The litigation hold files contain the names and email addresses of EPA employees and EPA contractors, interns, or grantees who have been provided EPA email addresses and who have been identified as custodians of information that needs to be preserved in the anticipation of litigation. The records in the system will include these individuals' names and EPA email addresses which are entered into the system by designated EPA employees responsible for the administration of litigation holds. Information in the system includes litigation hold notices and answers to certification questions. Reports may be generated from the system that identify whether an individual is designated as a custodian of hold-responsive information, as well as reports containing the information received from individuals in response to questions asked through the litigation hold system.

- **eDiscovery Case Tracking Files.**

The case tracking files contain information about the cases created in response to a litigation, investigation, FOIA matter or other formal information request. Case tracking files may contain the names, phone numbers, organizations, and email addresses of EPA employees and EPA contractors, interns, or grantees who have been identified as custodians in a case or as points of contact for managing the case. Information in the case tracking files may include the location of the information to be searched, search terms and case notes entered into the system by designated EPA employees or contractors responsible for operating EPA's eDiscovery Enterprise Tool Suite.

- **eDiscovery Collection Files.**

The collection files contain information potentially responsive to a litigation, investigation, FOIA matter or other formal information request. The Tool Suite may capture many types of personally identifiable information depending on where that information is stored, including an individual's name; work address and telephone number; home address and telephone number; email addresses; vehicle information; names of individuals associated with a FOIA request or litigation hold; or other related information. The collection files contain all data collected by the tools using the search criteria and may contain, but not be limited to, correspondence (e.g., case coordination reports; memoranda and other records of communication, including electronic communication over email systems or instant messaging among other EPA employees and/or personnel of other federal agencies and outside parties and attachments to those messages or communications); local/shared drive data; information collected or compiled from EPA database systems; spreadsheets of data collections often including personally identifiable information or law enforcement data used to track the process of investigations or focus investigative priorities; records relating to litigation by or against the United States government; records relating to requests for EPA records other than requests under the FOIA and the Privacy Act of 1974; legal documents including complaints, summaries, affidavits, litigation reports, motions, subpoenas and any other court filing or administrative filing, or other related litigation documents; documentary evidence; supporting documents related to the legal and programmatic issues of a case; transcripts of interviews; regulatory history (i.e., permits and reports generated as a result of normal program activity); administrative record material and comments on administrative records; technical support (reports generated to test search criteria); investigative notes; reports requesting permission

and use; transcripts of tapes; records checks (personal history, police information, fingerprint cards, photographs); property reports; property obtained and retained by an examiner including documents, personal property and documentary or other evidence; employment records and information related to employment matters; claims and records regarding discrimination, including employment and sex discrimination; personnel matters; contracts and information relating to contracts; manifests and other related investigative information.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There is a risk that the eDiscovery Enterprise Tool Suite may retain data longer than the sources systems' retention periods.

Mitigation:

This risk is mitigated through the implementation of the CIO Procedure 2155-P-03, *Collection and Retention Procedures for Electronically Stored Information (ESI) Collected Using E-Discovery Tools*. Further, if a litigation hold is in place, the normal disposition of records is suspended and the Agency must preserve this information until the hold is lifted.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Information produced from the RelativityOne Government Tool may be shared with external parties, as appropriate. In discovery matters, information may be shared with the Department of Justice or opposing counsel, as appropriate. For FOIA matters, information will be provided to the FOIA requester and subject to the nine FOIA exemptions for disclosure under the FOIA. Information from the system will be shared with a member of Congress or congressional staff in response to a congressional inquiry. Such disclosures are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes. EPA's General Routine Uses are published here:

<https://www.federalregister.gov/documents/2008/01/14/E8-445/amendment-to-general-routine-uses#h-14>.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The Agency will publish a SORN for the RelativityOne Government Tool indicating that EPA's General Routine Uses A, C, D, E, F, G, H, I, K, and L apply to this system. Refer to <https://www.federalregister.gov/documents/2008/01/14/E8-445/amendment-to-general-routine-uses> for a full explanation of these routine uses. The information collected via the RelativityOne Government Tool is used in a manner that is compatible and consistent with the purposes for which the information has been collected.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Disclosures of information residing in the RelativityOne Government Tool are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes.

4.4 Does the agreement place limitations on re-dissemination?

Disclosures of information residing in the RelativityOne Government Tool are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

There is a risk that a disclosure of information occurs in a manner not consistent with EPA's General Routine Uses.

Mitigation:

This risk is mitigated by restricting access to the system to authorized users, and further restricting access to user groups based on their particular functions and only to records responsive to their specific requests. Information will be shared for the stated purposes.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The RelativityOne Government Tool is used to preserve, collect and review information from source systems and maintain this information for the purpose of legal discovery or responding to FOIA requests, congressional inquiries or other official requests for

information. The ability to request the use of the RelativityOne Government Tool is limited to authorized requestors who are required to identify the purpose for their request to use of the system. Additionally, access to the records in the system is restricted to a limited number of authorized users with the appropriate security clearances and password permissions. Safeguards are presented in the limited access to the system that would help prevent unauthorized access which in turn ensure information is used in accordance to 6.1. EPA personnel and contractors are required to take the annual security training which includes privacy segment. To minimize the risk of compromising the information that is being stored in the system, strict access controls have been imposed. Access to the tool suite containing records is restricted to a limited number of authorized users with the appropriate security clearances and password permissions. Access to the system is further limited by user type. System administrators have full access to the tool suite, including the ability to perform administrative functions. Other users are provided a level of access to the tool suite that is commensurate with their role in the system, allowing them to perform the functions for which they are authorized. Authorized users include federal and contract staff located throughout the country. The system is maintained in secure areas and buildings with physical access controls. How the data is protected is outlined in the System Security Plan (SSP) in the control implementation statements. During the third party assessment for continued Authorization To Operate (ATO), these controls are audited in accordance EPA and federal policy.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The Agency's mandatory Information Security and Privacy Awareness Training contains information on the proper handling of PII data.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk that the required information privacy controls may not be implemented fully or correctly.

Mitigation:

This risk is mitigated through annual security assessments that are conducted to ensure compliance with privacy requirements.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The RelativityOne Government Tool will be used to respond to formal information requests in a variety of contexts including litigation, criminal investigations, FOIA requests, congressional inquiries and other formal requests for information from EPA by a variety of

requesters. The information collected via the RelativityOne Government Tool is used in a manner that is compatible and consistent with the purposes for which the information has been collected.

- 6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes X No . If yes, what identifier(s) will be used.** *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)*

Data in the system will be retrieved by custodian name and/or email address.

- 6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?**

No evaluation has been conducted. The information contained in the system is a copy of information that already resides on EPA's network of which there is no expectation of privacy for or for which the information was required to be provided to EPA under federal law, of which there is no expectation of privacy for.

- 6.4 Privacy Impact Analysis: Related to the Uses of Information**

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a risk that the information maintained in the RelativityOne Government Tool is used for purposes other than the purpose for which it was collected or the information is accessed by unauthorized users.

Mitigation:

This risk is mitigated by restricting access to the system and providing training. The uses of the information for the RelativityOne Government Tool are relevant and necessary for legal discovery and to respond to FOIA requests, congressional inquiries and other formal requests for information. To ensure information is handled in accordance with the uses described above, a limited number of individuals can request the use of the system for a particular matter and they are asked to identify the purpose for the request (e.g., litigation, FOIA, congressional inquiry etc.). Additionally, there are role-based access control for users of the system. Users are provided access to information in the system based on their need to know. Individuals working on a particular matter will be given access only to the information related to that matter. The technical team and system administrators are given full access to information in the system to perform technical and administrative functions. The system is maintained in secure, access-controlled areas and buildings. Users of EPA systems are required to complete security and privacy training on an annual basis to ensure continued access to the system.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

An individual identified as a custodian of information in a litigation, FOIA, congressional or other matter may or may not be notified in advance of a collection of their electronically stored information (ESI).

However, when a user of an EPA computer logs onto his/her computer, he/she is provided with a government warning notice which states,

“In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following:...4) you have no reasonable expectation of privacy regarding any communications or information used, transmitted, or stored on U.S. Government information systems; 5) at any time, the U.S. Government may for any lawful government purpose, without notice, monitor, intercept, search, and seize any authorized or unauthorized communication to or from U.S. Government information systems or information used or stored on U.S. Government information systems; 6) at any time, the U.S. Government may for any lawful government purpose, search and seize any authorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information; 7) any communications or information used, transmitted, or stored on U.S. Government information systems may be used or disclosed for any lawful government purpose, including, but not limited to, administrative purposes, penetration testing, communication security monitoring, personnel conduct measures, law enforcement, and counterintelligence inquiries...”

A SORN for the RelativityOne Government Tool will be published in the Federal Register to provide written notice of the Agency's intent to collect information from individuals for the purpose of legal discovery or responding to a FOIA request, congressional inquiry or other official request for information.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

There are no opportunities for individuals to consent to uses, decline to provide

information or opt out of the collection or sharing of the information.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

There is a risk that the individual may not be aware that information is being maintained in the RelativityOne Government Tool.

Mitigation:

Adequate notification is provided on point of collection.

8.1 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures for identifying the records to be changed and the corrective action sought are described in EPA's Privacy Act regulations at 40 CFR part 16 (<https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bc49ed29ef09e5d4e4fee&mc=true&node=pt40.1.16&rgn=div5>).

8.2 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.