United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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 Roster.docx

System Name: RelativityOne Government		**System Owner: Carolyn Scully**	
Preparer: Justin Burrows		**Office:** Office of Finance and Administration (OFA) / Office of the Chief Information Office (OCIO) / Data and Enterprise Programs Division (DEPD) / eDiscovery Branch (EDB)	
Date: 3/5/2026		**Phone:** 202-566-1457	
Reason for Submittal:			
New: ☐	Revised:☐	Annual Review: ☑	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☑	Rescindment/Decommission: ☐		

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 OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

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

The RelativityOne Government ("RelOne Gov" or "ROG") Software-as-a-Service ("SaaS") eDiscovery cloud-based tool enables the U.S. Environmental Protection Agency ("EPA" or "the Agency") to ingest, search, analyze, and produce large amounts of data that may be relevant to support discovery in litigation, FOIA, congressional inquiries, enforcement matters, or other disclosure of document requests, as mandated by law and EPA policy. RelativityOne Government uses many of its core capabilities to accomplish discovery functions, such as data transfer, data ingestion and structuring, search, document

review and coding, and production and export.

RelativityOne Government assists attorneys, FOIA professionals, and other EPA staff in reviewing records about a specific case/matter in a central, secure "workspace" (document review repository) per case/matter. After the results of a search/collection are downloaded from an EPA source repository, they are loaded to a RelativityOne Government workspace. Authorized end-users are then provided access to that secure workspace, wherein the documents are reviewed for responsiveness to the request, and a determination is made as to whether the documents can be released or should be withheld, either partially or in full. Once the end-users' review is complete, the documents are exported from the RelativityOne Government platform in PDF format by the eDiscovery Branch and copied to a secure location for end-users to access/download.

RelativityOne Government is currently hosted within the Microsoft Azure Government cloud. This system is an enterprise offering, run by a Working Capital Funded service, Discovery Services, which is managed and operated by the eDiscovery Branch ("EDB"). EDB prepared this Privacy Impact Assessment because RelativityOne Government will collect, use, and maintain personally identifiable information ("PII"). Due to the nature of eDiscovery data collection and processing, various types of PII will potentially be collected to support FOIA, litigation, congressional inquiries, enforcement matters, and other document/information requests. Such PII includes contact information of EPA staff, contractors, grantees, and non-EPA individuals who communicate with the Agency. Data within RelativityOne Government is collected from EPA enterprise repositories (e.g., M365, network locations, ECMS/ARMS, legacy Lotus Notes mailboxes, and local computers/workstations) or provided to the EDB via GoAnywhere, the Agency's internal file transfer platform.

The eDiscovery Branch also utilizes RelativityOne Government's Legal Hold application. The Legal Hold application is an integrated solution for complete, customizable, and semi-automated management of litigation holds, assisting components of EPA in complying with litigation hold obligations.

Section 1. 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.

- 40 U.S.C. Chapter 25 - Information Technology Management (Clinger-Cohen Act of 1996, also known as the Information Technology Management Reform Act of 1996).
- 44 U.S.C. Chapter 33 - Disposal of Records.
- 44 U.S.C. Chapter 35 - Coordination of Federal Information Policy (Paperwork Reduction Act of 1980, as amended, Paperwork Reduction Reauthorization Act of 1995, and Government Paperwork Elimination Act).
- 5 U.S.C. § 552 – Freedom of Information Act (as amended).
- Fed. R. Civ. Proc. 26 – Federal Rules of Civil Procedure.

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?

Yes. The system has been issued an ATO. This Authorization to Operate will expire on September 9, 2027.

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.

An Information Collection Request is not 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 is maintained and stored in the RelativityOne Government cloud environment (FedRAMP Moderate: SaaS), which leverages the Microsoft Azure Government cloud (FedRAMP High: SaaS, IaaS, PaaS).

Section 2. 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).

The data contained within the RelativityOne Government platform may contain multiple categories of information that could be considered PII. The information is not directly sorted or organized based on any of these categories. PII may be contained within a document or file that is uploaded into a secure workspace for analysis and review of pending formal document disclosure activities.

General Categories of Information that May Be Personally Identifiable	Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	The information relates to: A. EPA 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	Comments
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 the litigation, FOIA, investigation, or other formal document disclosure process for which this system is used for.
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.

General Categories of Information that May Be Personally Identifiable	Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	The information relates to: A. EPA 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	Comments
Family members	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.
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 medicate or health information	X	A, B, C, D	See comment above.
Financial account information	X	A, B, C, D	See comment above.
Credit score	X	A, B, C, D	See comment above.
Credit card numbers	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	X	A, B, C, D	See comment above.
Salary information	X	A, B, C, D	See comment above.
Legal documents	X	A, B, C, D	See comment above.

General Categories of Information that May Be Personally Identifiable	Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	The information relates to: A. EPA 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	Comments
Device identifiers, e.g., mobile devices	X	A, B, C, D	See comment above.
Foreign activities	X	A, B, C, D	See comment above.
Insurance information	X	A, B, C, D	See comment above.
Travel information	X	A, B, C, D	See comment above.
Criminal records information (arrests, charges …etc)	X	A, B, C, D	See comment above.
Civil law enforcement information	X	A, B, C, D	See comment above.
Whistleblower	X	A, B, C, D	See comment above.
Grand jury information	X	A, B, C, D	See comment above.
Information concerning witnesses to criminal matters	X	A, B, C, D	See comment above.
Procurement/contracting records	X	A, B, C, D	See comment above.
Propriety 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	X	A, B, C, D	See comment above.
Voice records/signature	X	A, B, C, D	See comment above.
Scars, marks, tattoos	X	A, B, C, D	See comment above.
DNA Profiles	X	A, B, C, D	See comment above.
System audit data	X	A, B, C, D	See comment above.
User ID	X	A, B, C, D	See comment above.
User Password/codes	X	A, B, C, D	See comment above.

General Categories of Information that May Be Personally Identifiable	Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	The information relates to: A. EPA 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	Comments
IP address	X	A, B, C, D	See comment above.
Date/time of access	X	A, B, C, D	See comment above.
Queries run	X	A, B, C, D	See comment above.
Content of files accessed or reviewed	X	A, B, C, D	See comment above.
Contents of files	X	A, B, C, D	See comment above.
Other (please list the type of info and describe as complete as possible:)	X	A, B, C, D	Given the purpose of RelativityOne Government, any PII relevant and necessary to EPA litigation, FOIA, investigations, and other disclosure activities could be maintained in this system, including PII not otherwise within the referenced categories of this table.

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

The sources of information for the RelativityOne Government document review platform are from EPA's Microsoft environment (M365) and/or EPA file repositories (e.g., legacy Lotus Notes mailboxes, ECMS, ARMS, and network or cloud storage locations), and hardware (workstations). The information is collected using EPA's Microsoft tool (Purview) and/or PinPoint Labs' Harvester, an eDiscovery collection tool. Or information may be provided to the EDB via GoAnywhere, the Agency's internal file transfer platform. Information is not collected directly from the public or non-EPA systems.

For RelativityOne Government's Legal Hold application, case attorneys identify the custodians who are subject to the hold, and case attorneys/Litigation Hold Administrators (LHAs) provide the litigation hold notice language, which describes custodians' obligations to preserve

information subject to the hold.

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.

2.4 Discuss how accuracy of the data is ensured.

The data retained in the RelativityOne Government document review platform are copies of information already residing in other EPA systems/repositories. Therefore, the accuracy of the data in the RelativityOne Government Tool depends on the accuracy of the data in the EPA source systems/repositories. The RelativityOne Government platform has validation and integrity checks to ensure data is not changed or modified in transit.

For the data within RelativityOne Government's Legal Hold application, it is the responsibility of case attorneys and Litigation Hold Administrators (LHAs) to ensure custodian information is accurate.

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:
In the process of collecting and reviewing information for its relevance to a matter within RelativityOne Government, there is a risk that privacy information is collected and reviewed.

Mitigation:
We deploy privacy controls from NIST SP 800-53 to secure PII. The information residing in the RelativityOne Government platform and the RelativityOne Government Legal Hold application are necessary for legal discovery and to respond to FOIA requests, enforcement matters, congressional inquiries and other formal document requests made to the Agency. To mitigate privacy risk, access to a RelativityOne Government workspace is restricted to end users who have been authorized by the requester, alternate requestor, or the workspace owner for that case/matter (see Section 3.1). Part of the review process includes withholding, or applying redactions to exempted information, such as privacy information, and/or applying document watermarks to limit distribution before exporting documents from the RelativityOne Government platform. Access to the RelativityOne Government Legal Hold application is restricted to authorized end users who have a need to know including, case attorneys, Litigation Hold Administrators (LHAs), and Records Liaison Officers (RLOs).

Section 3. 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?

Yes. Administrator access to the RelativityOne Government platform and the RelativityOne Government Legal Hold application is restricted to a limited number of authorized users within the eDiscovery Branch with the appropriate security clearances and permissions. End users must read and acknowledge the EDB-RelativityOne Government Rules of Behavior before gaining access to the RelativityOne Government platform. End users must reacknowledge and recertify their Rules of Behavior on an annual basis. End users may only access workspaces/databases in RelativityOne Government for which the requester, alternate requester, or workspace owner has explicitly granted access based on their need to know. Access to the RelativityOne Government document review platform is further limited by user type. Access to the RelativityOne Government Legal Hold application is restricted to case attorneys, Litigation Hold Administrators (LHAs), Records Liaison Officer (RLOs), and mobile device managers.

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

EPA's Access Controls applies to the Cloud Service Provider, Relativity, has implemented for RelativityOne Government are included in their System Security Plan ("SSP") and approved as part of the Agency Authorization to Operate ("ATO") and FedRAMP Authorization. The access controls the eDiscovery Branch are responsible for are specifically addressed in the system security plan EDB has developed for RelativityOne Government and other Branch standard operating procedures. These controls are assessed annually.

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

Authorized users of the RelativityOne Government document review platform include federal and contractor staff located in the eDiscovery Branch, including eDiscovery technicians, case managers, and federal and contract staff supporting the eDiscovery Branch in OFA. End users reviewing collected data to determine the data's relevance to a particular case/matter will have access to the information maintained in the RelativityOne Government platform, as appropriate. These employees may be assigned to the various Agency Program Offices and Regions. On occasion, federal staff at external agencies such as the Department of Justice ("DOJ") are granted access to RelativityOne Government workspaces at the request of the workspace owner.

Authorized users of the RelativityOne Government Legal Hold application include federal and contractor staff located in the eDiscovery Branch, mobile device managers, and case attorneys, Litigation Hold Administrators (LHAs), Records Liaison Officers (RLOs) located throughout the Agency.

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?

Only authorized users of the RelativityOne Government platform have access. As described in section 3.1 and 3.3, authorized users of the RelativityOne Government document review platform include system administrators and end users who are federal and contract staff. Authorized users of the RelativityOne Government Legal Hold application include, case attorneys, Litigation Hold Administrators (LHAs), Records Liaison Officers (RLOs), and mobile device managers. In addition, users have multi-factor authentication credentials to access the RelativityOne Gov platform and the data within it. The appropriate FAR contract clauses, 52.224-1 Privacy Act Notification and 52.224-2 Privacy Act, have been incorporated into the contract.

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.

Information is retained for the length of time needed to respond to the matter the information is necessary for and/or based on EPA Record Schedules, specifically Schedule Nos. 1012, 0089, 1049, 1020, and 1025. The RelativityOne Government platform itself does not have an EPA Records Control Schedule.

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 RelativityOne Government platform may retain data longer than the source systems' retention periods.

Mitigation:
This risk is mitigated through the implementation of data management and retention procedures. We review record retention schedules periodically to ensure information is not retained beyond the authorized period.

Section 4. 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 governments, 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 exported from the RelativityOne Government platform may be shared with external parties, as appropriate. Information may be shared with the Department of Justice ("DOJ") or opposing counsel, as needed. The data shared by EPA allows DOJ to perform legal discovery in litigation involving EPA, along with investigative activities in enforcement matters referred to DOJ by EPA. Additionally, on occasion, federal staff at external agencies such as the Department of Justice ("DOJ") are granted access to RelativityOne Government workspaces at the request of the workspace owner. Data within the platform may be exported and/or shared with other federal agencies, as needed, for equity review to occur. Equity review is part of a FOIA or other document review process whereby organizations with equity ownership in a document are given the opportunity to review before release.

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

External sharing is compatible with the purposes of the original collection. The data is specifically collected for the purpose of being shared with DOJ for litigation activities, including legal discovery and official requests for agency information. In the instances of equity review, the sharing is necessary as part of the review process prior to release.

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?

Currently, no memoranda of understanding or information sharing agreements have been issued

for the RelativityOne Government platform.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable.

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 low risk that confidentiality and availability of information being shared with external agencies could be lost.

Mitigation:
This risk is partially mitigated by uploading the information to a designated, secured file transfer platform with password encryption when sharing data with the DOJ. Additionally, redactions and/or distribution watermarks may be used when sharing with another federal entity for purposes of equity review.

Section 5. 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 platform is used to review information for the purpose of legal discovery, enforcement efforts, and responding to FOIA requests, congressional inquiries or other official requests for information. The ability to request the use of the RelativityOne Government platform is limited to authorized requesters who must obtain their supervisors' approval and agree to the Rules of Behavior. Authorized requesters are required to identify the purpose for their request to use of the system (e.g., FOIA, litigation, congressional) (see Section 3.1). The system will be continuously monitored, and a privacy impact assessment will be performed as needed, such as the current instance.

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

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There is minimal risk related to auditing and accountability in terms of changes to the configuration of

the system, failure of the audit logging function, and verification of the accuracy of information processed.

Mitigation:

Audit logging functions are implemented correctly (e.g., no PII in audit record) and assessed periodically. The Agency's Privacy Office conducts periodic privacy impact assessments to evaluate risk to PII collected and processed, and advises on whether certain data are still required. The system collects PII relevant and necessary to accomplish the mission. Data is only collected and retained for the specific purpose. Only authorized administrators can effect changes to the configuration of the system.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

The RelativityOne Government platform is used to respond to formal information requests in a variety of contexts including litigation, enforcement matters, investigations, FOIA requests, congressional inquiries, and other formal requests for information from EPA. The information stored in the RelativityOne Government platform is used in a manner that is compatible and consistent with the purposes for which the information has been collected, namely, to identify responsive documents and redact/withhold information, as appropriate.

The RelativityOne Government platform also contains the Agency's Legal Hold application. The Legal Hold application is used to track the Agency's litigation holds and the custodians subject to those holds.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☑ 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.

The RelativityOne Government document review platform is designed to search the text of the documents that have been ingested for purposes of legal review or other document review. The system has the capacity to search on any word, term, phrase, or combination thereof to identify potentially relevant information within a secured workspace. Such searches cannot be conducted across all workspaces or the entire RelativityOne Government platform at once.

RelativityOne Government's Legal Hold application uses the custodian's name and/or email

address to retrieve the custodian's litigation hold status.

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?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

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 at the approval of the requester, alternate requester, or workspace owner. Users must abide by the access controls outlined in Section 3.1.

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 RelativityOne Government 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 platform are relevant and necessary for legal discovery, enforcement matters, and to respond to FOIA requests, congressional inquiries, and other formal requests for information.

To ensure information is handled only in accordance with these uses, a limited number of individuals can request the use of the system for a particular matter, and these individuals are asked to identify/validate the purpose for the request (e.g., litigation, FOIA, congressional inquiry, etc.). Additionally, there are role-based access controls in place for users of the system. Users are provided access to information in the system based on their need to know and only with the approval of the requester, alternate requester, or workspace owner. Individuals working on a particular matter will be given access only to the information related to that matter. The eDiscovery Branch's technical team and system administrators are given full access to information in the system to perform technical and administrative functions. Users of EPA systems are required to complete security and privacy training on an annual basis to ensure continued access to the system, as noted in Section 3.1.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

Information within the RelativityOne Gov platform is collected from other source systems in the Agency. No additional notice, beyond the existing CIO Policies and Procedures, including EPA's National Rules of Behavior, is provided.

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.

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 an individual may not be aware that information is being maintained in the RelativityOne Government platform.

Mitigation:
Notice is provided through EPA's National Rules of Behavior.

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 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 Freedom of Information Act (FOIA).

Privacy Risk:

None.

Mitigation:

None.

I attest as the Agency Privacy Officer that **RelativityOne Government (RelOne)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.05.08 10:33:47 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA