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: eDiscovery Enterprise Tool Suite		**System Owner:** Heather Thompson	
Preparer: Heather Thompson		**Office:** OFA/OCIO/DEPD/EDB	
Date: April 6, 2026		**Phone:** 202-566-1025	
Reason for Submittal:			
New: ☐	Revised: X	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X	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 eDiscovery Enterprise Tool Suite is a moderate system which operates under and is governed by EPA system controls and policies. The eDiscovery Branch (EDB) operates the eDiscovery Enterprise Tool Suite.

The eDiscovery Enterprise Tool Suite (eDiscovery) is a set of software tools and hardware hosted at EPA's National Computing Center (NCC) that EDB uses to search and collect EPA data from specific data sources at the request of its customers. The customers of this system primarily include EPA program staff and attorneys. The search and collection of EPA data is done in support of litigation, Freedom of information Act (FOIA) requests, Congressional inquiries, and investigative matters. The

types of data supported by the eDiscovery Enterprise Tool Suite include nearly all types of data created by users of EPA computers systems, including, but not limited to, email messages and attachments, word processing documents, spreadsheets, presentation files, portable document format (PDF) files, digital photos, images from mobile devices, scanned documents, etc. The eDiscovery Enterprise Tool Suite consists of three (3) applications – Harvester, Cellebrite and Data Warehouse.

Harvester

Harvester, an enterprise-wide eDiscovery collection tool, searches for and collects files and folders across the EPA network for the purposes of litigation, Freedom of Information Act (FOIA) requests, Congressional inquiries, and investigative matters. EDB uses Harvester to forensically collect data from source locations outside of the Microsoft Office 365 environment. EDB uses terminal server V18H1N-HARVEST to run the Harvester application. Data collected by Harvester is saved to/temporarily stored in collection shares until a copy of the data is exported/downloaded from the collection share and uploaded to RelOne Gov, a separate system with its own ATO, for processing and hosting.

Data Warehouse

The Data Warehouse tool is used as a QA/QC tool to ensure that duplicate case tracking identification numbers are not assigned to a search request. EDB maintains all assigned ED numbers in a SQL table on the V18H1N-DWSQL1 server. If an ED number already exists in the SQL table, the operator will be notified and will work with our intake/eDiscovery Assistance Team (eDAT) to find and assign a new ED number to the search request.

In addition, EDB uses Data Warehouse to create load files for its ROG database, a workspace in RelOne Gov used by EDB and its customers to obtain and track information about RelOne Gov review workspaces. The application uses application programming interfaces (APIs) created within the V18H1N-DWDEV1 server and loads the information into a table on the V18H1N-DWSQL1 server. A dat file is generated that includes fielded information that maps to fields in the Relativity ROG workspace.

Cellebrite

Cellebrite is a digital forensics tool used to access, extract, and analyze data from EPA-issued mobile devices. The tool offers a comprehensive and rapid extraction of data from a wide range of mobile devices, along with detailed reporting to assist in navigating and reviewing the data extracted from those devices. The mobile device image data is stored in an S3 bucket in the EPA AWS ECHS cloud and managed in accordance with Agency records schedules and EDB's device imaging data retention procedure.

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 eDiscovery Enterprise Tool Suite 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 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).

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, a security plan for the system was completed. Yes, the system has been issued an Authorization-to-Operate. The ATO expires **May 11, 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, images extracted from mobile devices using Cellebrite will be stored in the AWS ECHS cloud. The AWS cloud solution is FedRamp approved. This solution offers compute and storage and a pre-defined set of PaaS services.

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).

eDiscovery Collection Files. The collection files contain all information responsive to designated search criteria that relate to litigation, FOIA, Congressional inquiries, and investigatory matters. The information in the system will also contain all types of data created by users of EPA computers systems, including, but not limited to, email messages and attachments, word processing documents, spreadsheets, presentation files, PDF files, digital photos, images from mobile devices, scanned documents, etc.

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

The sources of information are custodian local workstations, network locations, EPA-issued mobile devices, collaboration tools, electronic records repositories, email, and source locations outside of the EPA Microsoft Office 365 environment. Information is extracted from its native source using the applications within the eDiscovery Enterprise Tool Suite, 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. The eDiscovery technical team also accepts information from authorized EPA project requesters to facilitate electronic search, retrieval and utilization. No information is independently collected from the public or non-EPA systems. Rather, the information in the system is collected from authorized project requesters for the purpose of facilitating electronic search, retrieval, and utilization.

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 resides in the eDiscovery Enterprise Tool Suite has been collected from other EPA systems or repositories 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 in other EPA systems or repositories. Therefore, the accuracy of the data in the eDiscovery Enterprise Tool Suite depends on the accuracy of the data in the EPA source systems or repositories. Data in the eDiscovery Enterprise Tool Suite are not collected from non-EPA systems. In addition, accuracy of the data residing in the eDiscovery Enterprise Tool Suite is maintained by controlling access to the records in the Tool Suite. Access is restricted to a limited number of authorized users with the appropriate security clearances and password permissions; access is further limited by user type.

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 stored in the eDiscovery Enterprise Tool Suite 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. Most of the collected ESI is temporarily stored on file shares within the

eDiscovery Enterprise Tool Suite system in accordance with Agency records retention requirements and until confirmation that the data was completely and accurately (1) imported to EDB's RelativityOne Government (RelOne Gov) review platform, another system managed by EDB under a separate ATO, or (2) delivered to the Department of Justice (DOJ) via secure file transfer protocols. The information residing in the eDiscovery Enterprise Tool Suite is necessary for legal discovery and to respond to FOIA requests, congressional inquiries and other formal document requests made to the Agency. Part of the review process includes determining relevance of the information and not all information will be determined relevant for the matter for which it was collected.

Mobile device images are stored in the AWS cloud. The mobile device images will be retained in accordance with Agency record schedules and the eDiscovery Branch's mobile device data retention policy. Mobile device images may be delivered to DOJ to support Agency litigation. DOJ will review the data for relevance and not all of the mobile device data will be determined relevant for the matter.

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?

Access to the eDiscovery Enterprise Tool Suite 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. Authorized users include federal and contract staff located in the eDiscovery Branch. 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 Control Procedure: CIO 2150-P-01.4.

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

Authorized users of the eDiscovery Enterprise Tool Suite include federal and contract staff located in the eDiscovery Branch. This includes eDiscovery technicians, case managers and federal and contract staff supporting the EPA Discovery Services Program.

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 eDiscovery Enterprise Tool Suite include federal and contract staff located in the eDiscovery Branch. This includes eDiscovery technicians, case managers, federal and contract staff supporting the Discovery Services Program.

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

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.

The collected ESI is retained in accordance with EPA Record Schedules, specifically Nos. 1012, 1006g, and 0089, and as necessary for responding to the matter. 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.

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 collected data longer than the sources systems' retention periods.

Mitigation:

EDB manages the collected ESI in accordance with the appropriate records retention schedule and, where applicable, legal hold requirements. EDB retains the collected ESI only as long as there is a business use for the collected data.

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 collected using the eDiscovery Enterprise Tool Suite may be shared with external parties, such as outside counsel, as appropriate. In discovery matters, collected data may be delivered to the DOJ and/or released to 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. Data collected using 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 has published a SORN for the eDiscovery Enterprise Tool Suite 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.

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 eDiscovery Enterprise Tool Suite 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 eDiscovery Enterprise Tool Suite 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 functions. Information will be shared for the stated purposes.

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 eDiscovery Enterprise Tool Suite is used to collect 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 eDiscovery Enterprise Tool Suite is limited to authorized requestors who are required to identify the purpose for their request to use 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.

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 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. 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 eDiscovery Enterprise Tool Suite will be used to collect data to support the Agency's response to formal information requests in a variety of contexts including litigation, criminal investigations, FOIA requests, congressional inquiries, and other formal requests for information. The information collected via the eDiscovery Enterprise Tool Suite 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 collected using the Harvester tool will be temporarily stored by custodian name on file shares maintained at the NCC until the data is loaded to RelOne Gov, a system owned/operated by EDB under a separate ATO and PIA or delivered to the DOJ. Data collected using the Cellebrite tool will be temporarily stored on local desktops maintained by the EDB Device Imaging Unit (EDB DI) and a virtual machine maintained at the NCC until the data is moved to the AWS cloud and/or delivered to the DOJ. EDB DI will retrieve data from the AWS cloud by

custodian name in response to a data collection request received by the DOJ.

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.

EPA has not conducted a formal evaluation of the effect of the privacy of the individuals whose information may be maintained in the system of records. The eDiscovery Enterprise Tool Suite collects data from other systems, such as EPA email and OneDrive accounts, SharePoint sites, and network drives. The data collected is maintained on file shares on an intermediary basis to transfer the data to a workspace within the RelOne Gov platform for Agency staff to review the documents, or to the DOJ. EPA maintains a separate ATO and PIA for the RelOne Gov application. Data collected using the Cellebrite tool will be temporarily stored on local desktops maintained by the EDB DI and a virtual machine maintained at the NCC until the collected data is moved to the AWS cloud and/or delivered to DOJ.

Most of the information contained in the eDiscovery Enterprise Tool Suite is from the EPA employee's email, EPA-issued mobile device, and other work-related document repositories. The impact or effect of the privacy of individuals is minimal at best since most of the information originated from the individual's EPA issued accounts.

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 eDiscovery Enterprise Tool Suite 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 collected by the eDiscovery Enterprise Tool Suite 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 controls 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 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.

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. Discovery Services provides document collection and review services for matters wherein the Agency is required by law or statute to respond.

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 was collected and is being maintained in the eDiscovery Enterprise Tool Suite.

Mitigation:

This risk is mitigated through the SORN and PIA for the eDiscovery Enterprise Tool Suite and the SORNs and PIAs for the source systems of the information.

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:

There is a risk that information believed to be inaccurate or erroneous cannot be corrected in the system, rather the information should be corrected in the source system.

Mitigation:

This risk is mitigated through the notice provided in the SORN for the source systems of information and the procedures for seeking corrective action described in EPA's Privacy Act regulations at 40 CFR part 16 (https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bcdc49ed29ef09e5d4e4fee&mc=true&node=pt40.1.16&rgn=div5).

I attest as the Agency Privacy Officer that **eDiscovery Enterprise Tool Suite (eDiscovery)** 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 13:08:48 -04'00'

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