

Date of Approval: 12/05/2025  
Questionnaire Number: 2598

## Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

OpenText Encase Information Assurance- eDiscovery

Acronym:  
IA

Business Unit  
Information Technology

Preparer  
# For Official Use Only

Subject Matter Expert  
# For Official Use Only

Program Manager  
# For Official Use Only

Designated Executive Representative  
# For Official Use Only

Executive Sponsor  
# For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

OpenText Encase Information Assurance is a dedicated software used by IRS IT Electronic Discovery Program Office to perform forensic investigations and Electronic Discovery process across the network. The IRS needs this software to make all reasonable efforts and due diligence to search, identify, collect, preserve, and process electronically stored information in the custody of the IRS from Outlook mailboxes, removable media, workstations, databases, home directories and more. We need this software to provide thousands of attorneys' data allowing them to prepare for trials. Not being able to access this data in a timely manner would make it impossible to meet statutorily and judicially imposed deadlines, putting tens of billions in revenue at risk. EnCase Information Assurance v24.x is designed to address the needs of forensic and electronic discovery consultants at law firms or corporations, attorneys, and paralegal professionals. OpenText

EnCase Information Assurance provides enterprises with 360-degree visibility across all endpoints, devices, and networks to search, collect and preserve electronically stored information (ESI) discreetly and in a court-admissible format. It performs discrete targeted collections on a multitude of sources, including on-premises systems, cloud repositories and distributed endpoints, complete with reporting, auditing, and logging to ensure chain of custody.

## Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

EnCase Information Assurance v24.x is designed to address the needs of forensic and electronic discovery in Litigation Hold process for law firms/ corporations, attorneys, and paralegal professionals or fulfillment of FOIA responsibilities. OpenText EnCase Information Assurance provides enterprises with 360-degree visibility across all endpoints, devices, and networks to search, collect and preserve electronically stored information (ESI) discreetly and in a court-admissible format. It performs discrete targeted collections on a multitude of sources, including on-premises systems, cloud repositories and distributed endpoints, complete with reporting, auditing, and logging while ensuring chain of custody. The application/ system has no authority to dispose the collected data. The data can only be removed once the Chief Counsel completes the Litigation and issues the Litigation Hold Releases which would be authoritative directive for litigated related data disposition.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address  
Adoption Taxpayer Identification Number  
Agency Sensitive Information  
Email Address  
Employer Identification Number  
Employment Information  
Federal Tax Information (FTI)  
Individual Taxpayer Identification Number (ITIN)  
Name  
Preparer Taxpayer Identification Number (PTIN)  
Procurement Sensitive Data  
Protected Information

Social Security Number (including masked or last four digits)  
Tax ID Number  
Telephone Numbers

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

PII for personnel administration - 5 USC

SSN for personnel administration IRS employees - 5 USC and Executive Order 9397

SSN for tax returns and return information - IRC section 6109

## Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system? (Number)

2

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

7404

4.12 What is the previous PCLIA title (system name)?

OpenText Encase Information Assurance, eDiscovery

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

Expiring PCLIA

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

No SDLC - this is upgrading existing systems as we do upgrade every year.

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Enterprise Operations (EOPS) because this is server-client application, and the infrastructure is mostly comprised of back-end servers.

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (<https://ea.web.irs.gov/aba/index.html>) for assistance.

211187

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

No

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

All Examiners in IT electronic discovery only has Read and Modified access to the examining data set.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

IRM 34-007-001-2018-08-13 - specifically IRM 34.7.1.1.4.3.3 bottom of page 19; Chief Counsel Notice CC 2009-024; CCDM 34.7.1 attached; IRM 25.3.1 Litigation and Judgements - General Guidelines. In addition, daily logon banner also gives you warning that this is government system, and it is subjected to be monitored and to be collected data. Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

50,000 to 100,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Under 50,000

22 How is access to SBU/PII determined and by whom?

We have multiple layers of access to operate the system/ and its application. Only members in ITEDISCOVERY Case Examiners (8-10 IT Specialists) positions would need to request few Business Entitlement Access Request System (BEARs) entitlements. The entitlements would have to go through Infrastructure and System technical Lead, and Manager (First/ Second Level of Approvers) to determine the access should be approved or denied if necessary. After that those entitlements would go to System Admin/ Exchange Admin and or M 365 Admin who would authorize to grant the request entitlements. You would need to be several different roles in eDiscovery Examiner such as Purview eDiscovery Examiner; Azure Admin Role, Exchange PowerShell cmdlet, Encase User; Exchange Admins to access in performing the process of examining the cases with necessary access to complete results for Litigation Hold Requests. In addition, each examiner are specifically assigned to processing Virtual Machines

that delegate access by Infrastructure Lead. These processing virtual machines are not for personal use, only for case processing.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

Audit trail will provide job targets, Examiners who work on the cases, case number, custodian involved, date and time stamp of the job. Sample is in attachment section.

27 Does this system use or plan to use SBU data in a non-production environment?

No

## Interfaces

### Interface Type

IRS Systems, file, or database

### Agency Name

eDiscovery data repository, M365 Purview application, then Information Assurance process data

### Incoming/Outgoing

Both

### Transfer Method

Application to Application (A2A)

### Interface Type

IRS Systems, file, or database

### Agency Name

Privileged Access Workstation; Processing virtual machine, M365 Purview application to application.

### Incoming/Outgoing

Both

### Transfer Method

Application to Application (A2A)

### Other Transfer Method

# Systems of Records Notices (SORNs)

## **SORN Number & Name**

IRS 48.001 - Disclosure Records

Describe the IRS use and relevance of this SORN.

We are under obligation to be in compliant in providing records as requested by Litigation Hold or any other legal processes.

## **SORN Number & Name**

IRS 36.003 - General Personnel and Payroll Records

Describe the IRS use and relevance of this SORN.

These records are provided as directed and requested from Chief Counsel; TIGTA or Others in fulfilling obligation to comply with litigation hold or Freedom of Information Act (FOIA) process.

## **SORN Number & Name**

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

These data set results are provided to Chief Counsel/ or Treasury Inspector General for Tax Administration (TIGTA) to be in compliant with Litigation Hold request process as we are obligated to observe.

# Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.1: General Technology Management Records

What is the GRS/RCS Item Number?

010

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Information Technology (IT) infrastructure, systems, and services project records document the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes requirements for and implementation of functions such as:

- maintaining network servers, desktop computers, and other hardware,
- installing and upgrading network operating systems and shared applications, and

- providing data telecommunications; and infrastructure development and maintenance such as acceptance/authorization of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with implementation, modification, and troubleshooting.

Includes installation and testing records

- installation reviews and briefings
- quality assurance and security review
- requirements specifications
- technology refresh plans
- operational support plans
- test plans
- models, diagrams, schematics, and technical documentation

Exclusion: Records relating to specific systems that support, or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of a records schedule to NARA.

Note: Records concerning the development of each information technology (IT) system and software application are covered under the item for System Development Records.

What is the disposition schedule?

Temporary. Destroy when 5 years old, but longer retention is authorized if needed for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.1: General Technology Management Records

What is the GRS/RCS Item Number?

011

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

These records relate to the development of information technology (IT) systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving. Includes records such as:

- project plans
- feasibility studies
- cost analyses
- requirements documents
- compliance documents including:

- o Privacy Threshold Analyses (PTAs)
- o Privacy Impact Assessments (PIAs)
- o Security Plan
- o Information Protection Plan
  - change control records
  - Project Schedule
  - Plan of Action and Milestones (POA&M)
  - Configuration Management Plan
  - Resource Management Plan
  - Risk Assessment/Mitigation Plan
  - Security Plan
  - Disaster Recovery Plan
  - Test /Acceptance Plan
  - Quality Control Plan
  - Deployment Guide
  - User Guide
  - Training Guide

Exclusion: This item does not apply to system data or content.

Note 1: For certain technical documentation (e.g., data dictionaries, file specifications, code books, record layouts, etc.) related to the detailed, as-built design or maintenance of an electronic system containing permanent records, use the GRS item Documentation Necessary for Preservation of Permanent Electronic Records.

Note 2: This is consistent with the fact that the most complete version of system documentation is retained within the maintenance phase.

What is the disposition schedule?

Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

061

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process. Included are policies and procedures planning records; stand-up

configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records. Policies and procedures planning records relate to defining and establishing PKI systems. Records relate to such activities as determining that a PKI should be established; creating project implementation plans; creating the certificate policy (CP), certification practice statement (CPS), and other key operating documents; developing procedures in accordance with the CP and CPS; conducting risk analyses; developing records management policies (including migration strategies); and selecting the entity that will serve as registration authority (RA).

What is the disposition schedule?

Temporary. Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

060

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

PKI administrative records. Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process. Included are policies and procedures planning records; stand-up configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records.

What is the disposition schedule?

Temporary. Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.

## Data Locations

What type of site is this?

Shared Drive

What is the name of the Shared Drive?

Shared Drive for Electronic Discovery Request (SHREDR)

What is the sensitivity of the Shared Drive?

Sensitive But Unclassified (SBU)

What is the URL of the item, if applicable?

Not Applicable because we have 25 shared drive Servers commonly known as SHREDR since they are named with SHREDR and number in the systems' names.

Please provide a brief description of the Shared Drive.

These shared drives are functioned as our data center which are storing our data collections, preservation data sets, processing data set as well as Data Result set servers. These are secure servers, and they are not available for public shared drive. They are dedicated to use only for electronic discovery purposes.

What are the incoming connections to this Shared Drive?

Our privileged access workstation (PAW) to collect and to upload to these SHREDR or our electronic discovery processing virtual machines to process and to upload result data set to Result servers.

What are the outgoing connections from this Shared Drive?

Chief Counsel specific attorneys have access to the data set in the Result servers for their specific electronic discovery request cases.