Date of Approval: **February 25, 2020**

PIA ID Number: **4685**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Encase eDiscovery, eDiscovery

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Encase eDiscovery, eDiscovery PIA #2129

What is the approval date of the most recent PCLIA?

3/20/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

We were upgraded and migrated encase eDiscovery from old version 5.15 to version 6.01

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

IT:EOPS:ETI:TISO:IT eDiscovery Enterprise Technology Implementation (ETI) Technology Implementation Services Office (TISO)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The Encase eDiscovery (electronic discovery) module is used to preserve, to process and to present accordingly to the Litigation Hold Requests initiated by Chief of Counsel organization. The eDiscovery process assisted our Enterprise to defend litigations/ and to avoid civil and monetary sanctions by Courts.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

We in IT eDiscovery are only in compliant with Litigation Hold Requests from Chief of Counsel. Sometimes, there will be some instances which SSN usage is required to identify entities.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The use of SSN in litigation Hold Request process is unavoidable because those are unique fields to identify involved parties in the litigation hold process. Very infrequently, requested search terms from Chief of Counsel may contain SSN, Name or EIN of entities involved in the Litigation process. The system/ application is not widely used but it is restricted and limited usage to Examiners in eDiscovery organization primarily to support the Litigation Hold process.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Standard Employee Identifier (SEID)

Biometric Identifiers

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Procurement sensitive data Contract proposals, bids, etc.

Protected Information Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Are there other types of SBU/PII used in the system?

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

All Litigation Hold Requests are initiated by Chief of Counsel and if there are any SBU/ PII data requested, they are limited only in regard to litigation hold process only. Sometimes, search terms in litigation hold memo may contain EIN/ SSN and other SBU information and the use of these SBU/PII are completely relevant and limited to Chief of Counsel requests only. All SBU/ PII data sets are stored on secured servers with access limited to only those involved to support Litigation Hold process only. All processed data are securely contained

in Encase LEF (Logical Evidence File) format to protect confidentiality, integrity and non-repudiation of the data.

How is the SBU/PII verified for accuracy, timeliness and completion?

The system does verify the accuracy of the data. The data is searched based on criteria provided by Office of Chief Counsel litigation hold request memo which is legal documentation. The Encase application is widely used and accepted by Legal Community in Forensics and eDiscovery fields. All processed data are securely contained in LEF Logical Evidence File format to demonstrate confidentiality, integrity and non- repudiation of the evidences.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 00.002 Correspondence Files: Inquiries about Enforcement Activities

IRS 48.001 Disclosure Records

IRS 90.003 Chief Counsel Litigation and Advice (Criminal) Records

IRS 90.002 Chief Counsel Litigation and Advice (Civil) Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Ediscovery Scans custodian and Outlook for only litigation hold request relevant information for each case request.
Current PCLIA: No
SA&A: No

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: . Form Name: Ediscovery Scans custodian and Outlook for only litigation hold request relevant information.

Form Number: . Form Name: Ediscovery Scans custodian and Outlook for only litigation hold request relevant information.

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

Yes

Please identify the form number and name:

Form Number: . Form Name: Ediscovery Scans custodian and Outlook for only litigation hold request relevant information.

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the authority

The systems do not directly disseminate SBU/ PII to other IRS systems, but our direct customers are from Chief of Counsel organization from which litigation hold requests were sent to us. We processed and delivered results to Chief of Counsels. The results are saved on secured servers with restrictive role-based access.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

The notice is provided with official Litigation Hold Request initiated from Chief of Counsel. The memo then was sent to Business Unit Manager to contact employee for notifications of what Litigation Hold is about and he or she is subjected to data collection and all other details such as date range, data collection request and others information in regard to Litigation Hold.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

Data is collected from the employee laptops, workstations, and server and any removable media which are identified as property of the US Government in accordance to the Hold Request memo.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

The Encase eDiscovery system does not directly interact with individuals. Due process is provided through established channels to meet rights of the individual. Encase eDiscovery only supports this process by meeting litigation hold requirements for Chief Counsel.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Read Write

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Only

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

Based on IRM 11.3.35.6 (3), employees are directed by Chief Counsel and the Commissioner to provide information in response to eDiscovery requests. Once IT receives an eDiscovery request (EDR) and establishes the source of the EDR to be from Government Counsel, the EDR memo is then noted as the evidence that the request is made by Government Counsel. All EDRs processed by the IT E-Discovery Office are officially triggered by a formal EDR memo from Office of Chief Counsel. As such, the designated IT personnel proceeds to capture data per the EDR Memo. Access to the data within the system is restricted to the EnCase Examiner and Chief Counsel personnel. Other IT personnel

simply collect the data, but do not spend time analyzing the data itself. The Examiners and Counsel staff will have access to any and all data pertinent to a set search criteria. The user's profile and roles are assigned by his/her manager which is reviewed System Administrator and established when user accounts are created. A user's position and need-to-know determines the level of access to the data. The System Administrator grants approval for system access. A user's access to the data terminates when the user no longer required access. Criteria, procedures, controls, and responsibilities regarding access are document in IRS access control documentation.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

The Encase eDiscovery application is non-recordkeeping and National Archives approval is not required to affect data disposition. Information collected in response to eDiscovery searches are copies of information obtained from other IRS electronic repositories. Information will be maintained in the Encase eDiscovery application long enough to satisfy delivery of relevant information and/or transfer to a data server repository for official recordkeeping purposes (and disposed of in accordance with those files). GRS 5.1 Item 020-Non-recordkeeping copies of electronic records-Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

EnCase eDiscovery uses audit trails as required by IRS 2.1.10, Information Systems Security, May 1998, and a Functional Security Coordinator is assigned. Risk assessments have been performed in accordance with the following guidelines: TD P-71-10 Security Manual, TD P 85-03 Risk Assessment Guidelines. Also, Encase eDiscovery provides activity logs as well.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

We went through all application functionalities tests including actual processing steps, criteria, and job scheduling to validate each steps which have been functioned as it is designed to protect information privacy, integrity and confidentiality.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

We went through all application functionalities tests including actual processing steps, criteria, and job scheduling to validate each steps which have been functioned as it is designed to protect information privacy, integrity and confidentiality.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Not Applicable

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

There may be some occasions that other non-cases related documents being collected or captured because the requirement is almost always stating "all user created files" related to the legal matter. So, we only process based upon the criteria indicated in the Chief of Counsel Litigation Hold Request.

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

No