Date of Approval: **December 16, 2020**

PIA ID Number: **5623**

SYSTEM DESCRIPTION

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

Chief Counsel E-Discovery Litigation Support Service, CC eDisc LSS

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?

Software as a Service (SaaS) E-discovery #3142

What is the approval date of the most recent PCLIA?

12/12/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

Chief Counsel E-Discovery: Litigation Support Services (CCEdiscLSS)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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

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

Yes

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.

Electronic discovery or e-discovery refers to electronically stored information captured for legal proceedings, such as litigation, government investigations, or Freedom of Information Act requests. This is a FedRAMP-approved Software-as-a-Service (SaaS) cloud product that performs as a web-based document review and management software. It is used by corporations, the federal government, and law firms during the discovery phase of litigation. It is a highly scalable solution that stores, produces, and processes electronic evidence for tax court proceedings. The application is used by IRS end-users to manage litigation needs for multiple steps in the Electronic Discovery Reference Model (EDRM) framework. All documentation originates from taxpayers or their counsel, Department of Justice, or Department of Treasury. These include e-mails, documents, spreadsheets and images of other items submitted for evidence.

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)

Another compelling reason for collecting the SSN

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

See also 6.e below. Documents containing SSNs may be required to be produced in a tax trial or pretrial discovery response.

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

Redaction where necessary and appropriate

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

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Mother's Maiden Name

Protection Personal Identification Numbers (IP PIN)

Internet Protocol Address (IP Address)

Criminal History

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Alien Number

Financial Account Numbers

Photographic Identifiers

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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Procurement sensitive data Contract proposals, bids, etc.

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Proprietary data Business information that does not belong to the IRS.

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.

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

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 tax returns and return information is Internal Revenue Code Section 6109

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

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 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.

Documents containing PII and SBU information can be relevant to a tax litigation matter or discovery response. Such documents would be included in the tool to be reviewed and properly redacted before release to appropriate parties.

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

The documents and the content of those documents are created in other systems such as e-mail clients or word processing applications. Counsel employees are trained to handle SBU/PII in accordance with the Internal Revenue Manual (IRM) and other government regulations.

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 48.001 Disclosure 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?

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?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Opposing Counsel
Transmission Method: Electronic or Physical Media
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1041 Form Name: U.S Income Tax Return for Estates and Trust

Form Number: 1040 Form Name: U.S. Individual Income Tax Return

Form Number: 1065 Form Name: U.S. Return of Partnership Income

Form Number: 1120 Form Name: U.S. Corporation Income Tax Return

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

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

No

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

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Department of Justice
Transmission Method: Electronic media
ISA/MOU: Yes

Organization Name: Department of Treasury
Transmission Method: Electronic media
ISA/MOU: No

Identify the authority.

SBU/PII is disseminated by Department of Justice, Department of Treasury. Internal Revenue Code IRC Â§6103(h)(1) and IRC Â§6103(h)(2).

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

IRS 48.002

For what purpose?

The purpose is to process cases for the IRS as required by law.

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

3/15/2016

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

High

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage

Transmission

Maintenance

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?

Notice is provided via official IRS communication methods.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

Yes, if data is from taxpayer, they have the option to redact documents containing PII or SBU prior to release to IRS. No, if individual is subject to a litigation hold and data relevant to the matter is in their custody, they are obligated by the Federal Rules of Civil Procedure or the Tax Court Rules of Procedure to preserve and turn over any such data.

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

Information access and handling is restricted to the designated personnel working on each case. Due process is included in all IRS transactions per the guidelines of U.S. Code: Title 26 of the INTERNAL REVENUE CODE.

INFORMATION PROTECTION

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

Contractor Owned and Operated

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

IRS Employees

Users: Read Write

Managers: Read Write

IRS Contractor Employees

Contractor System Administrators: Administrator

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

Access to the system is role based and determined by the user's specific duties and strictly based on a need-to-know basis.

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.

All records copied to the system from IRS sources are copies of records that will be managed for GRS/RCS purposes in their original systems. The copies will be erased or purged from the system when no longer required to be preserved under the applicable litigation rules and other applicable legal requirements. Any records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedule (RCS) 13 for Counsel, Items 5-11, Case Files, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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.

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the necessary IRS personnel.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

The system is a cloud based solution and will follow the Managed Service path under the Enterprise Life Cycle (ELC). The need for a system test plan is To Be Determined.

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: More than 100,000

Contractors: More than 10,000

Members of the Public: More than 1,000,000

Other: Yes

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

The number of individual records provided above is only an estimate, the specific amount is not subdivided by source.

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?

Yes

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? Contact Disclosure to determine if an accounting is required.

Yes