
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Software as a Service (SaaS) E-discovery, CC eDisc SaaS

2. Is this a new system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

- No Vision & Strategy/Milestone 0
- No Project Initiation/Milestone 1
- No Domain Architecture/Milestone 2
- No Preliminary Design/Milestone 3
- No Detailed Design/Milestone 4A
- Yes System Development/Milestone 4B
- No System Deployment/Milestone 5
- No Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. 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 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. Please note: All forms of documentation are subject to discovery.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

- Yes Social Security Number (SSN)
- Yes Employer Identification Number (EIN)
- Yes Individual Taxpayer Identification Number (ITIN)
- Yes Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
- Yes Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers). The system is secured at the item level and only authorized persons are allowed to view the PII. If the PII in the document is to be shared, the information is redacted and only shared on a need to know basis for each case.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
Yes	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	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.
Yes	Proprietary data	Business information that does not belong to the IRS
Yes	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
Yes	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

- Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
- Yes SSN for tax returns and return information is Internal Revenue Code Section 6109
- Yes SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
- Yes PII for personnel administration is 5 USC
- Yes PII about individuals for Bank Secrecy Act compliance 31 USC
- Yes Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

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

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. 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.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treas/IRS 48.002	Disclosure Records

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Department of Justice (DOJ), Tax Court, Treasury	Electronic upload via media storage	Yes

11c. Does the system receive SBU/PII from State or local agency (s)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Opposing Counsel	Electronic or Physical Media	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

<u>Form Number</u>	<u>Form Name</u>
1041	U.S Income Tax Return for Estates and Trust
1040	U.S. Individual Income Tax Return
1065	U.S. Return of Partnership Income
1120	U.S. Corporation Income Tax Return

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? No

12b. Does this system disseminate SBU/PII to other Federal agencies? Yes

If **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)

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Department of Justice	Electronic media	Yes
Department of Treasury	Electronic media	Yes

Identify the authority and for what purpose? SBU/PII is disseminated by Department of Justice, Department of Treasury. The purpose is to process cases for the IRS as required by law under the authority of Internal Revenue Code IRC §6103(h)(1) and IRC §6103(h)(2).

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No
15. Does the system use cloud computing? Yes
16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

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

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information? Notice is provided via official IRS communication methods.

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

18a. If **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.

19. 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.

I. INFORMATION PROTECTION

20. 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
21. The following people have access to the system with the specified rights:

IRS Employees? Yes

<u>IRS Employees?</u>	Yes/No	Access Level (Read Only/Read Write/Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	No	
Developers	No	

<u>Contractor Employees?</u>	<u>Yes/No</u>	<u>Access Level</u>	<u>Background Invest. Level</u>
Contractor Employees?	<u>Yes</u>		
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	High
Contractor Developers	No		

21a. 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title. All records housed in the SaaS system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system's audit trail. The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the necessary IRS personnel.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **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.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: More than 100,000
26b. Contractors: More than 10,000
26c. Members of the Public: More than 1,000,000
26d. Other: Yes

If **other**, 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 currently available.

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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

If **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

End of Report
