

NOTE: The following reflects the information entered in the PIAMS Website.

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: 04/17/2014 PIA ID Number: 823

---

1. What type of system is this? Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Encase eDiscovery version 5, Encase eDiscovery v5

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

Enterprise Forensics and eDiscovery (EnCase)

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Under 100,000

---

4. Responsible Parties:

NA

---

5. General Business Purpose of System

---

The Encase eDiscovery v5 solution is a major application that has been procured by Cybersecurity and is currently supported by Information Technology Services, Business Relationship and Service Delivery. Due process is provided pursuant to the federal rules for criminal and civil process.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved:  / /

---

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) Yes
  - System is undergoing Security Assessment and Authorization Yes
- 

6c. State any changes that have occurred to the system since the last PIA

The Encase eDiscovery v5 has its own computer servers and SQL databases independent from the EnCase CyberSecurity solution.

---

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

---

## B. DATA CATEGORIZATION

---

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

**9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:**

Taxpayers/Public/Tax Systems	<u>No</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>No</u>	<u>Other Source:</u> <u>TIGta Records</u>

**10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:**

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	Yes
Tax Payer ID Number (TIN)	Yes	Yes	Yes
Address	Yes	Yes	Yes
Date of Birth	No	No	No

**Additional Types of PII:** No

**PII Name On Public? On Employee?**

No                  No

**10a. Briefly describe the PII available in the system referred to in question 10 above.**

Employee names, SEID, SSN, POD, home address and taxpayer name, address, Case number, etc.

**If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.**

**10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)**

IRM 11.3.35.6 (3) authorizes the IRS E-Discovery business processes. The information collected and managed by the IRS is of extremely high value for the agency and the Treasury Department. eDiscovery stores information protected under the Privacy Act of 1974. Such information is categorized as SBU. In addition, the Commissioner of the IRS has designated that all IRS systems and associated data can be categorized as SBU and protected under IRC 6103. And, being directed by Chief Counsel and the Commissioner to provide this information. E-Discovery and Litigation Hold ESI activities normally fall under the Federal Rules Civil Procedures and are not subject to FOIA or Disclosure rules and procedures. Based on IRM 11.3.35.6 (3), once the request is established to be from Government Counsel, there is no need to contact or work through Disclosure. The E-Discovery request memo from the Office of Chief Counsel is the evidence that the request is made by Government Counsel. All EDRs processed by the MITS E-Discovery Office are officially triggered by a formal memo from Chief Counsel.

**10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)**

Data collected and search results will be temporarily stored in the EnCase Logical Evidence File format and hosted on servers managed by EOPS. Then exported by Chief Counsel's staff in standard formats for legal analysis using review tools, such as Clearwell. Also, the files are named based the EDR

tracking number that correlates to specific litigation cases.

---

**10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?**

Risk Assessments have been performed in accordance with the following guideline: IRM 2.1.10 IS Security, TD P 71-10 Security Manual, TDP 85-03 Risk Assessment guideline.

**11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.**

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.

**11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes**

---

**12. What are the sources of the PII in the system? Please indicate specific sources:**

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

g. Other: No If Yes, *specify*:

---

**C. PURPOSE OF COLLECTION**

*Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use*

**13. What is the business need for the collection of PII in this system? Be specific.**

The Encase eDiscovery v5 solution is a major application that has been procured by Cybersecurity and is currently under deployment by the IRS supported by the Information Technology Services, Business Relations and Service Delivery. The information searched and collected is provided by the IRS employee computers, workstations, laptops, servers, business applications, and external media. A previous CII Number: MITS:CPP:ITSSP:EnCase-REQ-PIA-V1.0.0-022511 was granted for the Enterprise Forensics & eDiscovery (EnCase).

---

**D. PII USAGE**

*Authority: OMB M 03-22 & PVR #16, Acceptable Use*



---

**E. INFORMATION DISSEMINATION**

---

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

\*\* Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

*If other, specify:*

---

**F. INDIVIDUAL CONSENT**

---

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

18a. If Yes, how is their permission granted?

---

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent	Yes _____
Website Opt In or Out option	No _____
Published System of Records Notice in the Federal Register	No _____
Other: <u>Data is derived from the employee laptops, workstations, and server and any removable media which are all property of the US Government.</u>	Yes _____

---

**G. INFORMATION PROTECTIONS**

---

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

---

**21. Identify the owner and operator of the system:** IRS Owned and Operated

**21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?**

---

**22. The following people have use of the system with the level of access specified:**

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>No Access</u>
Developers		<u>Read Only</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>Read Only</u>
Contractor System Administrators		<u>Read Only</u>
Contractor Developers		<u>Read Only</u>
Other:	<u>No</u>	

**If you answered yes to contractors, please answer 22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

---

**22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?** Yes

**23. How is access to the 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 a 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.

---

**24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?**

Not applicable. The system does verify the accuracy of the data. The data is searched based on criteria provided by Office of Chief Counsel.

---

**25. 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

---

**25a. 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.**

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).

**If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.**

---

**26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.**

Only authorized employees have access to the information on Encase eDiscovery. All employees and contractors receive UNAX and Code of Conduct training. Identification and access provisions are employed. All IRS personnel who have access will have organization specified clearances and are only granted access when their jobs require it. Their access is immediately revoked when it is no longer required. Access to the data within the system is restricted. Criteria, procedures, controls, and responsibilities regarding access are document in IRS access control documentation.

**26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.**

The System Administrator grants approval for system access. There are Audit Trails as required by IRS 2.1.19 Information Systems Security. Information retrieved by Encase eDiscovery is not consolidated, changed or modified in any way.

---

**27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes**

---

**28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.**

Encase eDiscovery does not receive any downloads or extract any data from any other source other than data input directly by tax examiners. There are Audit Trails as required by IRS 2.1.10 Information Systems Security and a functional Security Coordinator is assigned. All employees are required to attend UNAX Training and ther have been trained on the use of the system and their responsibilities concerning access and the use of the data. Risk assessments have been performed in accordance tithe guidelines. (IRM 2.1.10, TDP 71-10 Security Manual)

---

**29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Not Applicable**

---

**29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? Yes**

**29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?**

---

## **H. PRIVACY ACT & SYSTEM OF RECORDS**

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

---

**30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes**

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

**SORNS Number**

**SORNS Name**

Treas/IRS 24.030 IMF

Treas/IRS BMF

Treas/IRS 48.001 disclosure records

Treas/IRS 00.001 correspondence

Treas/IRS 34.037 Audit Trail and Security Records

**Comments**

## I. ANALYSIS

---

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

---

**32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?**

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

**32a. If Yes to any of the above, please describe:**

Not Applicable

[View other PIAs on IRS.gov](#)