

Date of Approval: April 17, 2017

PIA ID Number: **2265**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Electronic Recovery and Access to Data, ERAD

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Electronic Recovery and Access to Data, ERAD 1861

Next, enter the **date** of the most recent PIA. 11/14/2016

Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? Yes

If yes, explain what changes were made. Removed any mention of using the system to seize funds

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

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	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 Recovery and Access to Data (ERAD) is a service which allows IRS Criminal Investigation (CI) to query the balances of prepaid access devices. Prepaid access devices is a general term for prepaid debit cards, cash cards and gift cards. IRS can only query cards by account number; the system does not have the ability to query by name or other PII. IRS-CI will currently only allow the use of ERAD for tax related identity theft investigations and money laundering investigations where IRS-CI has a warrant signed by a judge (i.e., search warrant with the requisite language in the items to be seized).

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.)? No

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.

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

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

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)
No	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	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 this criteria. Be specific.

Electronic Recovery and Access to Data (ERAD) is a patented platform available only to Law Enforcement Agencies. This complete investigative solution provides law enforcement with the ability to inventory and interrogate any cash card found during a search warrant. ERAD has the ability, right at the point of the search, to determine the value of the card. The ERAD platform will be used to build evidence in investigations of alleged criminal activity associated with money laundering, identity theft and other financial crimes. IRS-CI will only use ERAD with an appropriate search warrant. However, case law does not require a search warrant to query card balances. Scanning of the card does not constitute a search under the Fourth Amendment. Unlike Demand Deposit Account (DDA) checking accounts where consumers' money is held in an individual bank account registered in their own name, prepaid card funds are held in an omnibus pooled account owned by a corporation. Prepaid card value is tracked by card number with the actual currency comingled in a single account owned by a company or financial institution. Since these funds are held in pooled accounts owned by corporations, and the customer does not have any equitable and legal title to that account, the prevailing opinion is that there are no expectations of privacy. According to United States v. Alabi, 943 F.Supp.2d 1201 (D.N.M. 2013), the swipe of the card to inquire about a balance is not a "search" of a card and therefore the 4th amendment does not apply. Furthermore, according to United States v. Benjamin, 2014 WL 5431349 (D.Neb. 2014), a scan of magnetically-coded information on a credit or debit card does not involve a physical intrusion into a constitutionally protected area. Nor, when the card is already in the physical possession of the person scanning it, is the magnetic strip a constitutionally-protected area. No contrary opinion has been found by any of the Courts which have considered this issue.

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

IRS-CI is committed to ensuring that its law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals. As part of this commitment, IRS-CI operates in accordance with rules, policies and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information

collected through the use of the ERAD Platform. It should be noted that IRS-CI does not share data collected from the ERAD system, however IRS-CI does work closely with other federal, state and local law enforcement partners and provides technological assistance under a variety of circumstances, such as in joint federal grand jury investigations. IRS-CI's policy ensures individual rights are not violated, as ERAD use requires appropriate authorization as well as a court order.

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>
IRS 46.005	Electronic Surveillance and Monitoring 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? No

11c. Does the system receive SBU/PII from State or local agency (-ies)? 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>
IRS does not own or control this database and is only a user.	Any agreements would be between ERAD and any entity which has agreements with ERAD.	No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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? No

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? Yes

If **yes**, identify the other source(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>
Government Officials	Various	No

Identify the authority and for what purpose? Special agents are authorized by 26 USC §6103(k)(6) to disclose return information to the extent such disclosure is necessary in obtaining information which may be relevant to a tax investigation, but is not otherwise reasonably available. These disclosures are called "investigative disclosures." A situation in which a special agent may have to make such a disclosure could arise when an agent contacts a third party believed to have information pertinent to a tax investigation and the information is not otherwise reasonably available.

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

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? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

IRS-CI will currently only allow the use of ERAD for investigations where IRS-CI has a warrant signed by a judge (i.e., search warrant with the requisite language in the items to be seized). This warrant will be provided to the person who physically possesses the cards.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? The searches and seizure of data and funds are court ordered via search or seizure warrant.

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

(1) Rule 16 affords pre-trial opportunities for the government and the defense to examine evidence in the opposing party's possession, custody, or control. (2) The government or a defendant can, by using a subpoena duces tecum, compel the pre-trial production of evidentiary material per Fed. R. Crim. P. R17(c).

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)

IRS Owned and Operated

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

IRS Employees? Yes

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

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Prior to deployment of the technology, use of ERAD by IRS-CI must be approved by a Special Agent in Charge (SAC). IRS-CI personnel must be trained and supervised appropriately. ERAD may be operated only by trained personnel who have been authorized to use the technology and whose training has been administered by the manufacturer or a qualified agency component or expert. All CI employees are required to complete annual ethics training and are prohibited from using IRS systems for non-business purposes.

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? No

22b. 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.

ERAD is the owner of the data and the IRS is not able to dictate record retention policies. Any data retrieved from the system would be part of the agents case file, _____ and generally maintained 10 years after case closed as required by IRM 1.15.30 for Criminal Investigation, Item 15.

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? Do not know

23.1 Describe in detail the system s audit trail. ERAD retains all queries for a period of 7 years.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. IRS does not own or control the system

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:	<u>Not Applicable</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>More than 1,000,000</u>
26d. Other:	<u>No</u>

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? No

End of Report
