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: January 16, 2015 PIA ID Number: **1068**

1. What type of system is this? Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

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

Electronic Fraud Detection System , EFDS

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

3. Identify how many individuals the system contains information on

Number of Employees:	Under 50,000
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties: N/A

5. General Business Purpose of System

The Electronic Fraud Detection System (EFDS) is a mission critical, stand-alone automated system designed to maximize fraud detection at the time tax returns are filed to eliminate the issuance of questionable refunds. The EFDS detects reliable indicators of taxpayer fraud, keying highly focused investigations prior to the issuance of the refund. Due process is provided outside the system by titles 18 and 26, and the Federal Rules of criminal Procedure.

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: 12/11/2013

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 No

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

Added an IRS database connections required to implement ACA and ID Theft related processes. Added a new data element (Device ID).

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). 015-45-01-12-01-2221-00-315-180

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

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	Yes
Employees/Personnel/HR Systems	Yes
Other	No

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	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Telephone Number	Yes	Yes
Income information	Yes	No
Type of Tax Return filed (1040, 1040A, 1040EZ)	Yes	No
Document Locator Number (DLN)	Yes	No
Source of filing (paper or electronic)	Yes	No
Tax filing status	Yes	No
Number of dependents	Yes	No
Employer name	Yes	No
Federal Employer Identification Number (FEIN)	Yes	No
Employer address	Yes	No
EFDS User ID	No	Yes
Fax number	No	Yes
Badge number	No	Yes
Operating system password (encrypted)	No	Yes
Application password (encrypted)	No	Yes
Scheme Development Center (SDC)	No	Yes
EFDS User login ID	No	Yes
Group ID	No	Yes
Service Center Code	No	Yes
Workstation ID	No	Yes
Program ID	No	Yes
Record ID	No	Yes
Table ID	No	Yes
System date	No	Yes
Action date	No	Yes
Run date	No	Yes
View date	No	Yes
Tax Examiner (TE) code	No	Yes
Query type	No	Yes
Record type	No	Yes

Action type	No	Yes
Event	No	Yes
Field name	No	Yes
Number of rows retrieved	No	Yes
Employer Identification Number (EIN)	Yes	No
Table changed	No	Yes
Electronic Filing Identification Number (EFIN) emp	Yes	No
Prisoner Inmate Number	Yes	No
Prisoner Incarceration date	Yes	No
Prisoner Work release date	Yes	No
Prisoner Fugitive code	Yes	No
Prison code	Yes	No
Prison Institution Name	Yes	No
Address list of prisons	Yes	No
Device ID	Yes	No

10a. What is the business purpose for collecting and using the SSN ?

EFDS collects and uses Taxpayers SSNs and TINs to assist the IRS with its fraud detection efforts and to meet mission critical needs.

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.)

The regulations/internal revenue codes that deal specifically with requiring taxpayers to provide their SSN or EIN to IRS are: IRC 6011; IRC 6109-1; 26 CFR Section 301.6109-1 6011 requires the return, and 6109-1 says you have to provide an SSN if you're required to file a return.

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

There are no alternative solutions available for using masking, truncation, or alternative identifiers due to the mission of the EFDS application which is to assist the IRS with meeting its fraud detection efforts.

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

N/A - please see response to Question 10c.

Describe the PII available in the system referred to in question 10 above.

Taxpayer: Telephone number; Income information; Document Locator Number (DLN); Type of return filed (e.g., 1040, 1040A, 1040EZ); Source of filing (paper or electronic); Tax filing status; Number of dependents; Employer name; Federal Employer Identification Number (FEIN); Employer name; Employer address; Device ID. Employee: Name; EFDS User ID, Telephone number, Fax number, Badge number, Operating system password (encrypted); Application password (encrypted); Scheme Development Center (SDC). Federal/State Bureau of Prisons: Electronic Filing Identification Number (EFIN) employer identification number; Telephone number; Address listing; Prisoner name; Prisoner Date of Birth; Prisoner SSN; Prisoner Inmate number; Prisoner Incarceration date; Prisoner Work release date; Prisoner Fugitive code; Prisoner Prison code; Prisoner Institution name; Address list of prisons; Prison institution record - Prison code, Institution name; Prison Address; Prison phone

number.

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.

Audit Trail Information: EFDS User login ID; Group ID; Service Center Code; Workstation ID; Program ID; Record ID; Table ID; System date; Action date; Run date; View date; Tax Examiner (TE) code; Query type; Record type; Action type; Event; Field name; Number of rows retrieved; DLN; Employer Identification Number (EIN); Table changed.

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:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
TPDS (Component of e-Services)	Yes	12/06/2013	Yes	02/28/2014
RRP (Reclassified as a Level 3 Non-FISMA reportable application)	Yes	06/09/2014	No	02/28/2014
IPM	Yes	03/12/2014	Yes	06/03/2014
IMF	Yes	09/07/2012	Yes	11/15/2012
BMF	Yes	03/18/2013	Yes	05/23/2013
IRMF	Yes	09/19/2012	Yes	11/02/2012
QRP	Yes	12/11/2013	Yes	06/02/2014
MeF	Yes	12/13/2012	Yes	03/12/2013
CADE2	Yes	11/04/2014	Yes	07/12/2012
GMF (Reclassified as a Level 3 Non-FISMA reportable application)	Yes	07/06/2011	Yes	03/19/2012
RRP (Reclassified as a Level 3 Non-FISMA reportable application)	Yes	06/09/2014	No	03/19/2012

b. Other federal agency or agencies: Yes

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

Federal Bureau of Prisons Department of Health and Human Services (HHS)

c. State and local agency or agencies: Yes

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

State Bureau of Prisons

d. Third party sources: Yes

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

Commercial public business telephone directory listings/databases are purchased by Criminal Investigation (CI) to contact employers for employment and wage information. CI updates this database manually with correct information.

e. Taxpayers (such as the 1040): Yes

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

g. Other: No

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.

EFDS is a mission critical, automated system designed to maximize fraud detection at the time that tax returns are filed to reduce the issuing of questionable refunds. All data items compiled by the EFDS are used to cross-reference and verify information that relates to potentially fraudulent tax returns. Each data element present is necessary to support the business purpose of the system. NOTE: The system also functions in training mode, where all of the data available in production is available for training. Only those users authorized to access the system in production are authorized to access it for training, with the same OL5081 process and other access controls in place, including audit trails. The training data remains within the secure EFDS environment.

D. PII USAGE

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

14. What is the specific use(s) of the PII?

To conduct tax administration	Yes
To provide taxpayer services	No
To collect demographic data	No
For employee purposes	No
Other:	No

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:

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? N/A

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? Not Applicable

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? Yes

19a. If **Yes**, how does the system ensure “due process”?

EFDS does not ensure due process because of its use in Criminal Investigation activities. However, “Due Process is provided outside the system by titles 18 and 26, and the Federal Rules of Criminal Procedure.”

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

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

Form 1040	U.S. Individual Income Tax Return
Form 1040A	U.S. Individual Income Tax Return
Form 1040EZ	Income Tax Return for Single and Joint Filers With No Dependents

20b. If **No**, how was consent granted?

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:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Write
Managers		Read Only
System Administrators		Read Write
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

23. How is access to the PII determined and by whom?

All access credential requests are enforced through the Online 5081 process for granting permissions to systems and applications used by IRS personnel. Employees must complete and submit an Online 5081 request for EFDS access. The form contains information on the permissions or role to be assigned to the account. The request is forwarded to the employee's manager (or Functional Security Coordinator) and the system administrator of the application for approval. The manager and system administrator review the Online 5081 request to ensure that the correct access privileges listed on the form correspond to the user's job requirements. If everything is accurate, both the manager and system administrator must electronically sign off on the form. As a final step, the requesting user must also sign off agreeing that access to the application is required. A user's access to the data terminates when it is no longer required.

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

Due to the nature of the EFDS application, all input data is accepted as received. The application does not have the capability to modify the data that is received. This is outside of the EFDS scope.

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.

Records Control Schedule (RCS) 30 for Criminal Investigation, Item 15 for Investigative Files and IRM 1.15.35, Tax Administration - Electronic Systems, Item 36 for EFDS provide approved disposition instructions for CI and EFDS records/data. Audit logs are maintained in compliance with IRM 10.8.3, Audit Logging Security Standards. EFDS data and input records are approved for destruction/deletion when 1 year old or when no longer needed for administrative, legal, audit, or other operational purposes whichever is sooner. Additionally, IRM 1.15.35, Item 36 also stipulates the destruction of EFDS output records (paper or electronic reports) when 1 year old or when the information is obsolete, superseded or no longer needed in current operations whichever is sooner; destruction of audit trail information transferred to tape after 7 years. Note: RCS 30 is published in Document 12990, IRM 1.15.35 will soon be transitioning from IRM publication to Document 12990 as RCS 35.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
EFDS follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest. EOPs SAs can only access information necessary to perform their job function. The application adheres to the SA&A and physical security requirements set forth in IRM 10.4.1- Physical Security Program- Managers Security Handbook.

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

The EFDS Application interfaces protect PII in transit through the use of Enterprise File Transfer Utility (EFTU) access control, audit and encryption capabilities.

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.

Testing is conducted annually to ensure the selected controls are functioning correctly. When testing of a security control reveals that the control is not functioning as expected, the control deficiency is documented in the system's plan of action and milestones (POA&M). All test results are documented and reported to Business Unit (BU) Security Project Management Office (SPMO). The security state of the application is then reported to the appropriate organizational officials annually as defined in Treasury Directives Policy (TDP) 85-01.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

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? 11/14/2014

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.

No SORN Records found.

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)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No