

Date of Approval: **December 07, 2020**

PIA ID Number: **5614**

## **SYSTEM DESCRIPTION**

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

Electronic Fraud Detection System, EFDS

*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?*

Electronic Fraud Detection System, EFDS, Operations & Maintenance

*What is the approval date of the most recent PCLIA?*

1/10/2018

*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.*

Strategic Development (SD)

*Current ELC (Enterprise Life Cycle) Milestones:*

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.*

The Electronic Fraud Detection System (EFDS), also known as the RRP Legacy Component (RRP LC), 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.

## 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)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

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).*

The Social Security Number (SSN) is the primary means of updating or querying the data by other internal systems. It is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct records are accessed by IRS systems or when research is done on fraud cases. In addition, the SSN is used to restrict access by complying with the Taxpayer Browsing Protections Act.

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

The Office of Management and Budget (OMB) Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The SSN is the significant part of the data being processed/received/disseminated by EFDS and required to identify an EFDS record.

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

Internet Protocol Address (IP Address)

Criminal History

Financial Account Numbers

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.*

**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.

**Criminal Investigation Information** Information concerning IRS criminal investigations or the agents conducting the investigations.

*Are there other types of SBU/PII used in the system?*

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Tax Return Income, Withholding, and Deduction information (Individual Master File/Business Master File); Tax Refund Amount; Document Locator Number (DLN); Type of Tax Returns Filed; Source of Tax Return Filing (paper or electronic); Tax Filing Status; Number of Dependents; Name of Dependents; Employer Name; Employer Tax Identification Number; Employer Address; Employer Telephone Number; Bank Account Information; Date of Death; Employee: Name; EFDS User Identification Number (ID), Telephone Number, Fax Number, Badge Number, Scheme Development Center (SDC); Electronic Filing Identification Number (EFIN), Federal/State Bureau of Prisons/Prisoner Information; Preparer Tax Identification Number (PTIN); Tax Return Preparer Name and Employer Identification Number (EIN); and Device Identification Number (Device ID).

*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

*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.*

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, including Taxpayer Identification Numbers (TINs), 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 On-Line 5081 (OL5081) process and other access controls in place, including audit trails. The training data remains within the secure EFDS environment.

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

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. The EFDS system receives data from multiple internal IRS systems which have their own verification process for data accuracy, timeliness, completeness and therefore EFDS assumes that the data is accurate, timely, and complete when it is provided by these internal IRS (Internal Revenue Service) systems.

## **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 22.061 Information Return Master File
- IRS 24.030 Customer Account Data Engine Individual Master File
- IRS 24.046 Customer Account Data Engine Business Master File
- IRS 42.021 Compliance Programs and Projects Files
- IRS 46.002 Criminal Investigation Management Information System and Case Files
- IRS 46.050 Automated Information Analysis System
- IRS 34.037 Audit Trail and Security 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?*

Yes

*Enter the files and databases:*

System Name: Third Party Data Store (TPDS) - Subsystem of e-Services  
Current PCLIA: Yes  
Approval Date: 8/7/2019  
SA&A: Yes  
ATO/IATO Date: 2/21/2018

System Name: Integrated Production Model (IPM)  
Current PCLIA: Yes  
Approval Date: 6/6/2019  
SA&A: Yes  
ATO/IATO Date: 4/1/2015

System Name: Business Master File (BMF)  
Current PCLIA: Yes  
Approval Date: 8/27/2018  
SA&A: Yes  
ATO/IATO Date: 1/29/2018

System Name: Return Review Program (RRP)  
Current PCLIA: Yes  
Approval Date: 12/6/2019  
SA&A: Yes  
ATO/IATO Date: 5/22/2020

System Name: Individual Master File (IMF)  
Current PCLIA: Yes  
Approval Date: 3/4/2020  
SA&A: Yes  
ATO/IATO Date: 11/26/2019

System Name: Modernized e-file (MeF)  
Current PCLIA: Yes  
Approval Date: 2/20/2019  
SA&A: Yes  
ATO/IATO Date: 4/3/2018

System Name: Generalized Mainline Framework (GMF) (FISMA Non-Reportable)  
Current PCLIA: Yes  
Approval Date: 10/6/2017  
SA&A: Yes  
ATO/IATO Date: 9/13/2012

System Name: Information Returns Master File (IRMF) - Subsystem of Information Returns Processing (IRP)  
Current PCLIA: Yes  
Approval Date: 3/16/2020  
SA&A: Yes  
ATO/IATO Date: 10/22/2015

System Name: Questionable Refund Program (QRP) -Subsystem of EFDS  
Current PCLIA: Yes  
Approval Date: 1/10/2018  
SA&A: Yes  
ATO/IATO Date: 3/27/2020

System Name: Selection and Analytic Platform  
Current PCLIA: Yes  
Approval Date: 10/23/2019  
SA&A: Yes  
ATO/IATO Date: 3/27/2020

*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?*

No

*Does the system receive SBU/PII from Taxpayer forms?*

No

*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?*

Yes

*Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.*

System Name: Return Review Program (RRP)  
Current PCLIA: Yes  
Approval Date: 12/6/2019  
SA&A: Yes  
ATO/IATO Date: 5/22/2020



System Name: CADE2  
Current PCLIA: Yes  
Approval Date: 4/14/2020  
SA&A: Yes  
ATO/IATO Date: 7/9/2019

System Name: Splunk Enterprise  
Current PCLIA: Yes  
Approval Date: 1/27/2020  
SA&A: Yes  
ATO/IATO Date: 3/28/2017

*Identify the authority.*

Internal Revenue Code Section 6109 authorizes the collection and use of SSN information.

*For what purpose?*

EFDS collects information from and disseminates information to IRS systems for the purposes of tax administration along with detecting and preventing both identity theft and fraudulent tax refunds under Internal Revenue Code (IRC) Sections 6001, 6011, 6012e(a).

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

No

*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?*

No

*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?*

The EFDS system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC (United States Code).

*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):*

The EFDS system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

The EFDS system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any others ensuing actions. Due process is awarded during any ensuing criminal investigation or civil action. Due process is provided pursuant to 26 USC and 18 USC.

## **INFORMATION PROTECTION**

*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

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

*IRS Employees*

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Only

*IRS Contractor Employees*

Contractor Developers: Read Only

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

All access credential requests are enforced through the Online 5081 (OL5081) process for granting permissions to systems and applications used by IRS personnel. Employees must complete and submit an OL5081 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 office administrator of the application for approval. The manager and office administrator review the OL5081 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.

## **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.*

Document 12990 Records Control Schedule (RCS) 30 for Criminal Investigation (CI) Records, Item 40 for Investigative Files and Document 12990 RCS 32, IRS Electronic Tax Administration (ETA), Item 36 for EFDS provide approved disposition instructions for CI and EFDS records and data. Audit logs are maintained in compliance with (Internal Revenue Manual (IRM) 10.8.1. 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, Document 12990, Item 40 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.

## **SA&A OR ASCA**

*Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?*

Yes

*What date was it completed?*

3/27/2020

*Describe the system's audit trail.*

The Audit Trail data elements and Information captured within EFDS are as follows: Audit Trail Information: EFDS User login Identification (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; Document Locator Number (DLN); Employer Identification Number (EIN); Table changed. The EFDS audit data is sent to the Security Audit and Analysis System (SAAS) on a daily basis for further analysis and review.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

Yes

*Is the test plan completed?*

Yes

*Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?*

DocIt

*Were all the Privacy Requirements successfully tested?*

Yes

*Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?*

No

*Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?*

Privacy Requirements were met when the EFDS system was established - Security Control Assessment (SCA) testing was conducted and EFDS was granted an Authorization to Operate (ATO). EFDS undergoes Annual Security Control Assessment (ASCA) testing conducted by Cybersecurity. The EFDS Application interfaces protect PII in transit through the use of Enterprise File Transfer Utility (EFTU); access control, audit and encryption capabilities. EFDS users are required to complete annual mandatory briefings including privacy awareness and training. Additionally, EFDS operates using IRS infrastructure and behind the IRS firewall and does not have any outside connections.

## **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: Not Applicable

Contractors: Not Applicable

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

Other: No

## **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?*

No