A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Electronic Fraud Detection System, EFDS

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 Fraud Detection System, EFDS, 1068

   Next, enter the date of the most recent PIA. 1/16/2015

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

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

   Were there other system changes not listed above? No

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
   No System Development/Milestone 4B
   No System Deployment/Milestone 5
   Yes Operations & Maintenance (i.e., system is currently operational)

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

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.
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.

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 Office of Management and Budget (OMB) memorandum M-07-16 requires that federal agencies develop a mitigation or elimination strategy for systems that use Social Security Numbers (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.

   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

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

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

<table>
<thead>
<tr>
<th>Selected</th>
<th>SBU Name</th>
<th>SBU Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Agency Sensitive Information</td>
<td>Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission</td>
</tr>
<tr>
<td>No</td>
<td>Procurement sensitive data</td>
<td>Contract proposals, bids, etc.</td>
</tr>
<tr>
<td>No</td>
<td>Official Use Only (OUO) or Limited Official Use (LOU)</td>
<td>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.</td>
</tr>
<tr>
<td>No</td>
<td>Proprietary data</td>
<td>Business information that does not belong to the IRS</td>
</tr>
<tr>
<td>Yes</td>
<td>Protected Information</td>
<td>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</td>
</tr>
<tr>
<td>No</td>
<td>Physical Security Information</td>
<td>Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities</td>
</tr>
<tr>
<td>No</td>
<td>Criminal Investigation Information</td>
<td>Information concerning IRS criminal investigations or the agents conducting the investigations.</td>
</tr>
</tbody>
</table>
6d. Are there other types of SBU/PII used in the system? Yes

If 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).

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

No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

No PII for personnel administration is 5 USC

No PII about individuals for Bank Secrecy Act compliance is 31 USC

No 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.

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.

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.

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.
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.

<table>
<thead>
<tr>
<th>SORNS Number</th>
<th>SORNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treasury/IRS 22.061</td>
<td>Information Return Master File</td>
</tr>
<tr>
<td>Treasury/IRS 24.030</td>
<td>CADE Individual Master File</td>
</tr>
<tr>
<td>Treasury/IRS 24.046</td>
<td>CADE Business Master File</td>
</tr>
<tr>
<td>Treasury/IRS 42.021</td>
<td>Compliance Programs and Projects Files</td>
</tr>
<tr>
<td>Treasury/IRS 46.002</td>
<td>Criminal Investigation Management System</td>
</tr>
<tr>
<td>Treasury/IRS 46.050</td>
<td>Automated Information Analysis System</td>
</tr>
<tr>
<td>Treasury/IRS 34.037</td>
<td>Audit Trail and Security Record Systems</td>
</tr>
</tbody>
</table>

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?  Yes

If yes, enter the files and databases.
<table>
<thead>
<tr>
<th>System Name</th>
<th>Current PIA?</th>
<th>PIA Approval Date</th>
<th>SA &amp; A?</th>
<th>Authorization Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Data Store (TPDS) - Subsystem of e-Services</td>
<td>Yes</td>
<td>11/03/2015</td>
<td>Yes</td>
<td>05/01/2014</td>
</tr>
<tr>
<td>Return Review Program (RRP)</td>
<td>Yes</td>
<td>06/23/2017</td>
<td>Yes</td>
<td>10/06/2017</td>
</tr>
<tr>
<td>Integrated Production Model (IPM)</td>
<td>Yes</td>
<td>03/30/2016</td>
<td>Yes</td>
<td>04/01/2015</td>
</tr>
<tr>
<td>Individual Master File (IMF)</td>
<td>Yes</td>
<td>02/28/2017</td>
<td>Yes</td>
<td>11/14/2016</td>
</tr>
<tr>
<td>Business Master File (BMF)</td>
<td>Yes</td>
<td>04/24/2015</td>
<td>Yes</td>
<td>02/25/2016</td>
</tr>
<tr>
<td>Modernized e-file (MeF)</td>
<td>Yes</td>
<td>02/23/2016</td>
<td>Yes</td>
<td>11/09/2015</td>
</tr>
<tr>
<td>Information Returns Master File (IRMF) - Subsystem of Information Returns Processing (IRP)</td>
<td>Yes</td>
<td>03/09/2017</td>
<td>Yes</td>
<td>10/22/2015</td>
</tr>
<tr>
<td>Questionable Refund Program (QRP) - Subsystem of EFDS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>10/22/2015</td>
</tr>
</tbody>
</table>

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?  
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?  
Yes

If yes, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Current PIA?</th>
<th>PIA Approval Date</th>
<th>SA &amp; A?</th>
<th>Authorization Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CADE2</td>
<td>Yes</td>
<td>11/06/2015</td>
<td>Yes</td>
<td>04/21/2015</td>
</tr>
<tr>
<td>Return Review Program (RRP)</td>
<td>Yes</td>
<td>10/06/2017</td>
<td>Yes</td>
<td>06/23/2017</td>
</tr>
</tbody>
</table>

Identify the authority and for what purpose?  
EFDS collects information from and disseminates information to IRS systems for the purposes of tax administration under Internal Revenue Code (IRC) Sections 6001, 6011, 6012e(a). Internal Revenue Code Section 6109 authorizes the collection and use of SSN information.

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?  
No
G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels?  **No**
   
   If **no**, Contact *Privacy for assistance with completing the Social Media PIA.*

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?  **No**

16. Does this system/application interact with the public?  **No**

   If **no**, when will the e-RA be conducted?

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?

   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).

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):

   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.

19. 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.

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:

<table>
<thead>
<tr>
<th>IRS Employees?</th>
<th>Yes/No</th>
<th>Access Level (Read Only/Read Write/Administrator)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Yes</td>
<td>Read and Write</td>
</tr>
<tr>
<td>Managers</td>
<td>Yes</td>
<td>Read and Write</td>
</tr>
<tr>
<td>Sys. Administrators</td>
<td>Yes</td>
<td>Read and Write</td>
</tr>
<tr>
<td>Developers</td>
<td>Yes</td>
<td>Read-Only</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contractor Employees?</th>
<th>Yes/No</th>
<th>Access Level</th>
<th>Background Invest. Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contractor Users</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractor Managers</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractor Sys. Admin.</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractor Developers</td>
<td>Yes</td>
<td>Read-Only</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

21a. 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.

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.

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.

### 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)? Yes

23a. If yes, what date was it completed? 6/23/2017

23.1 Describe in detail 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. EFDS is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

### J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If yes, is the test plan in process or completed? Completed

24b.3 If completed/ or in process, 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?

There is no use of live data during the development testing phase of the EFDS system changes. Privacy Requirements were met when the system was established and granted an Authorization to Operate (ATO). 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.

24b.1. If completed, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIt

24b.2. If completed, were all the Privacy Requirements successfully tested? Yes

24b.2 If completed, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No
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:  Not Applicable
   26b. Contractors:  Not Applicable
   26c. Members of the Public:  More than 1,000,000
   26d. Other:  No

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? Yes

   If yes, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable). EFDS is listed in the "Department of the Treasury - 2016 Annual Privacy Act and Data Mining Report" located at the following link: https://www.treasury.gov/privacy/annualreports/Documents/Annual_Privacy_and_Data_Mining_Report%20FY16.pdf

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

   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.

30a. If no, accounting of Disclosures risk noted. Contact Disclosure to develop an accounting of disclosures. Explain steps taken to develop accounting of disclosures process.

30b. If N/A, explain the Exemption and/or Disclosure s response.

End of Report