

Date of Approval: **March 04, 2020**

PIA ID Number: **4630**

SYSTEM DESCRIPTION

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

Individual Master File, IMF

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?

Individual Master File (IMF) # 2140

What is the approval date of the most recent PCLIA?

2/28/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

The Individual Tax Processing Engine (ITPE) project is taking the existing posting and analysis functionality and updating the current programming language.

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Sustaining Operations (SO) ESC

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 IMF application is a system that is used for individual tax administration. It receives individual tax information from various sources, processes the information and generates data for refunds. It consists of a series of batch runs, data records and files. The IMF system receives individual tax submissions in electronic format and processes them through a pre-posting phase, posts the transactions, analyzes the transactions and produces output in the form of Refund Data, Notice Data, Reports, and information feeds to other entities. After the implementation of the Customer Account Data Engine 2, CADE2 daily processing, IMF processes a daily processing cycle for individual tax submission.

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)

Delivery of governmental benefits, privileges, and services

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

The SSN is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct record is accessed. IMF continues to examine all new requests that state a need to access the SSN to ensure there is a specific requirement and business approval to access the SSN in order to perform official IRS functions.

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

Prior to any future connections to downstream systems the IRS will examine alternative solutions and work with system owners to try and mitigate the need for the SSN. In addition, the IRS will routinely review IMF SSN uses and continue to find ways to replace, mask, or truncate the SSN. With the deployment of the CADE 2 database, the IRS has implemented the use of a unique tax payer identification number, which reduces the use of the SSN as an internal system identifier. As a matter of practice, the Service will also continue efforts to reduce taxpayer risk associated with using the SSN by examining alternatives.

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

Protection Personal Identification Numbers (IP PIN)

Financial Account Numbers

Tax Account Information

Centralized Authorization File (CAF)

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

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

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

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

No

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

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

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.

The Personally Identifiable Information (PII) collected from the IRS 1040 Forms and all supplemental documentation filed along with an individual's tax information is used to validate an individual's taxes. CADE 2 IMF only use SBU/PII data that are necessary to assess the taxes. This includes the SSN since it is the one unique identifier that taxpayers have to identify themselves.

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

Taxpayers submit their tax returns and other tax forms either electronically or manually. The Individual Master File (IMF) is an application that receives data from an array of sources to aid the IRS with regard to those tax return submissions. The IMF system receives data from various systems which have their own verification process for data accuracy, timeliness and completeness. However, IMF also verifies the SSN and Name against Social Security records and verifies the address using 3rd party address software.

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 24.030 Customer Account Data Engine Individual Master File

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: Notice Delivery System (NDS)

Current PCLIA: Yes

Approval Date: 4/4/2019

SA&A: No

System Name: Individual Master File Notice Identification (IMF NOTICE ID)

Current PCLIA: Yes

Approval Date: 3/6/2017

SA&A: No

System Name: Generalized Mainline Framework (GMF)

Current PCLIA: Yes

Approval Date: 10/6/2017

SA&A: Yes

ATO/IATO Date: 7/21/2013

System Name: Return Review Program (RRP)

Current PCLIA: Yes

Approval Date: 12/6/2019

SA&A: No

System Name: Notice Review Processing System - Individual Master File (NRPS IMF)

Current PCLIA: Yes

Approval Date: 7/5/2018

SA&A: Yes

ATO/IATO Date: 11/13/2018

System Name: Audit Information Management System-Reference (AIMS-R)
Current PCLIA: Yes
Approval Date: 9/19/2018
SA&A: Yes
ATO/IATO Date: 8/22/2018

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: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 1/17/2018

System Name: Generalized Unpostable Framework (GUF)
Current PCLIA: Yes
Approval Date: 11/28/2017
SA&A: No

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: National Account Profile (NAP)
Current PCLIA: Yes
Approval Date: 3/21/2017
SA&A: No

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: Notice Delivery System (NDS)
Current PCLIA: Yes
Approval Date: 4/4/2019
SA&A: Yes
ATO/IATO Date: 11/13/2018

System Name: Individual Master File Notice Composition (IMF NOTICE COMP)
Current PCLIA: Yes
Approval Date: 3/6/2017
SA&A: No

System Name: Individual Master File Notice Identification (IMF NOTICE ID)
Current PCLIA: Yes
Approval Date: 3/6/2017
SA&A: No

System Name: Integrated Production Model (IPM)
Current PCLIA: Yes
Approval Date: 6/6/2019
SA&A: Yes
ATO/IATO Date: 4/1/2016

System Name: State Income Tax Levy Program (SITLP)
Current PCLIA: Yes
Approval Date: 6/17/2017
SA&A: No

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 10/14/2018

System Name: Notice Review Processing System - Individual Master File (NRPS IMF)
Current PCLIA: Yes
Approval Date: 7/5/2018
SA&A: No

System Name: Financial Management Information System (FMIS)
Current PCLIA: Yes
Approval Date: 10/5/2017
SA&A: Yes
ATO/IATO Date: 10/5/2017

System Name: Notice Prints Processing (NPP)
Current PCLIA: Yes
Approval Date: 5/4/2018
SA&A: No

System Name: Quarterly Bankruptcy Extract (QBE)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 10/14/2018

System Name: Audit Information Management Systems Reference (AIMS-R)
Current PCLIA: Yes
Approval Date: 9/19/2018
SA&A: Yes
ATO/IATO Date: 8/22/2018

System Name: Generalized Unpostable Framework (GUF)
Current PCLIA: Yes
Approval Date: 11/28/2017
SA&A: Yes
ATO/IATO Date: 12/11/2013

System Name: Customer Account Data Engine
Current PCLIA: Yes
Approval Date: 10/30/2019
SA&A: Yes
ATO/IATO Date: 1/11/2019

Identify the authority

The authority for processing taxpayer information is 5 U.S.C. 301 and 26 U.S.C. 7801.

For what purpose?

The purpose for sharing taxpayer information received by other IRS systems and processed by IMF is to assess and distribute tax returns. In the case of IDRS information from IMF is shared for the purpose of providing data so that IDRS can assess case statuses and notice issuance.

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

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: US Census Bureau
Transmission Method: Connect Direct
ISA/MOU Yes

Organization Name: Bureau of Financial Services (BFS)
Transmission Method: Connect Direct
ISA/MOU Yes

Organization Name: Social Security Administration
Transmission Method: Connect Direct
ISA/MOU Yes

Identify the authority

Title 26, United States Code (U.S.C.), Section 6103, Subsections (j) and (n)

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

Provides authority for the IRS to transmit federal tax information to other federal agencies to maintain and support the confidentiality of information in the system of records suspected of potential fraudulent activities and prevent, minimize, and remedy such activities.

For what purpose?

To maintain records of tax returns, return transactions, and authorized taxpayer representatives by verifying SSNs with SSA, distributing refunds for FBS, and providing statistics to the Census Bureau.

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?

Notice is provided to individuals by other IRS applications or through forms (e.g., 1040 forms) that interact directly with the taxpayer at the time of collection. Due Process is provided pursuant to 5 USC.

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):

IMF does not collect any information directly from taxpayers. All information that is maintained by IMF comes from the submission of 1040 forms submitted directly to the IRS through other IRS systems. Information from the 1040 forms is collected and stored. The 1040 forms provide taxpayers information regarding the opportunity to decline or consent to providing the information. Due Process is provided pursuant to 5 USC.

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

IMF is only a repository of taxpayer information submitted directly to the IRS through other IRS applications. IMF does not interact with taxpayers directly and thus "due process" is addressed by other IRS applications that directly interact with taxpayers. Any issues that are identified by these other means requires the submission of requests for changes to IMF through automated methods so an auditable record may be maintained. Due Process is provided to 5 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

System Administrators: Read Write

Developers: Read Write

IRS Contractor Employees

Contractor Developers: Read Write

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

All those with access must go through the Public Trust Clearance process before access is considered. Once cleared, they must complete the proper request forms before access to IMF is obtained. All access must be approved by the user's manager who reviews the access request form at the time of submission and on an annual basis. The system administrators/approvers will also verify group membership to ensure system rights are limited based on the employee or contractor's need-to-know in order to perform their official duties. For access to an environment where a new or modified system is being tested (i.e., a non-production supporting environment) users must complete the necessary SBU data training, complete an access request form, and in some cases as outlined by the requirements set forth within the Internal Revenue Manual (IRM), submit an elevated access letter that is approved by the Associate Chief Information Officer prior to granting access. Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

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.

IMF data is approved for deletion/destruction 30 years after end of processing year. These disposition instructions are published in Document 12990 under Records Control Schedule

(RCS) 29 for Tax Administration - Wage and Investment Records (Service Center Operations), Item 203 (1). (1) Record copy-30 years after end of processing year. RCS 29, Item 203 (2)-(2) Copies required for research-Destroy 2 years after end of processing year, or when no longer needed in current operations. RCS 19, Item 23 (1)-Magnetic Tape Maintenance Records/Record copy- Destroy when 3 years old. RCS 19, Item 23 (2)-Magnetic Tape Maintenance Records/Tape Operations Records-Destroy 1 year after completion of action. RCS 19 Item 29 (2)-Individual Master File/Customer Account Data Engine (CADE) Archiving JCL-(2) All other weekly updated tapes-Scratch after successful completion of third update cycle. RCS 17 Item 20-Tax Processing Systems and Administrative Systems Project Files. The development and testing environments for the ITPE project will adhere to RCS Schedules 17 and 19. Depending on the environment, data can be deleted within two cycles or after one year.

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?

11/26/2019

Describe the system's audit trail.

The SA&A controls are assessed annually in accordance with the Annual Security Control Assessment (ASCA) to ensure system security and privacy compliance. Vulnerability scans and policy checkers are routinely run and if a vulnerability is detected efforts are made to address the concern upon discovery. In addition, IMF development areas that utilize live data periodically review staff lists to ensure listed support personnel require the level of access requested.

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)?

The test results are documented in the End of Test Report (EOTR).

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?

The IMF system is going through a continuous System Test Plan due to its ongoing enhancements. Each enhancement has a different set of design requirements which includes security and privacy requirements that are assessed. The overarching privacy requirements are tracked in the Rational Requirements Tool and reviewed by the development team. The identified requirements will then be tested and documented. Any risks that are discovered are reviewed and addressed. All this is being coordinated by Requirements Engineering Program Office and Cybersecurity and tracked in the Rational Requirements Tool and developer security assessment testing. The overarching privacy requirements are tracked in the Rational Requirements Tool. This is documented in the Planned Maintenance Requirements Checklist.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

3/21/2019

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

With the IMF containing all individual taxpayer data the capability does potentially exist where it can be used to identify, locate, and monitor individuals, especially through certain reports that can be generated. However, this is not the intent and the application that have the potential to produce such reports is audited and only a select few IRS employees will have this ability. In addition, the amount of content that can be pulled at any one time is limited in size in order to restrict such capabilities.

Does computer matching occur?

Yes

Does your matching meet the Privacy Act definition of a matching program?

Yes

Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Yes

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?

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.

Yes