Date of Approval: **August 03, 2020**

PIA ID Number: **5196**

## SYSTEM DESCRIPTION

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

Electronic Master File Transcript Requests (ELEC M, EMFTRA

*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 Master File Transcript Requests (ELEC MFTRA) EMFTRA PCLIA 2575, EMFTRA

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

8/17/2017

*Changes that occurred to require this update:*

Addition of Personally Identifiable Information (PII)

*Were there other system changes not listed above?*

Yes

*What were those changes?*

Due to retirement of Win 7 the replacement machine is a Win 10 - FRS001MA4329543

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

Sustaining Operations Executive Steering Committee (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?*

No

## 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 California Franchise Tax Board (FTB) customer sends requests for tax transcripts to the IRS via the Secure Data Transfer server (SDT) in order to match Federal taxpayer data to California taxpayer data. Tax Transcripts extracted from the IRS computers are routed to the IRS FTB workstation where a Disclosure officer reviews the transcripts and redacts information per Disclosure policies. The redacted tax transcripts are then sent to the California FTB using SDT. This data exchange increases Taxpayer Compliance.

## 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:*

Security Background Investigations

Interfaces with external entities that require the SSN

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

The SSN is used to match the taxpayer to state tax records for state tax administration purposes.

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

What the service is currently planning to replace the SSN is unknown, but they indicated that they are looking at replacing the SSN. Currently there is no alternative to the use of the SSN. The SSN is the significant part of the data being processed and there is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

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

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*

Official Use Only (OUO) or Limited Official Use (LOU) 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.

*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.*

Business Tax Returns

*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.*

To conduct tax administration. To provide taxpayer services. To collect demographic data. SSN's (or tax identification numbers) are necessary as this is how the State of California Franchise Tax Board requests records for matching taxpayer information against California records.

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

The Remittance Transaction Research (RTR) system receives data from the Integrated Submission and Remittance Processing (ISRP), Remittance Strategy for Paper Check Conversion (RS-PCC), and Lockbox Bank systems, which have their own verification process for data accuracy, timeliness, completeness and; therefore, RTR assumes that the data is accurate, timely, and complete when it is provided by these 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 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

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: Remittance Strategy for Paper Check Conversion (RS-PCC):
Current PCLIA: Yes
Approval Date: 9/23/2016
SA&A: Yes
ATO/IATO Date: 10/27/2015

System Name: Integrated Submission and Remittance Processing (ISRP):
Current PCLIA: Yes
Approval Date: 1/25/2017
SA&A: Yes
ATO/IATO Date: 1/27/2017

*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?*

Yes

*Please identify the form number and name:*

Form Number: IRS B.5.E  Form Name: 1040

*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?*

No

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

No

*Does this system disseminate SBU/PII to State and local agencies?*

Yes

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

Organization Name: California Franchise Tax Board
Transmission Method: Secure Data Transfer
ISA/MOU Yes

*Identify the authority*

California Franchise Tax Board receives the information described in this PIA under a memorandum of understanding as described below. Internal Revenue Service / California Franchise Tax Board Transcript Delivery System - 11/24/2004. The California Franchise Tax Board is the only state that receives this data.

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

PIAID 4702 IRC 6103(d) Tax Administration.

*For what purpose?*

Tax Administration

*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 system uses data entered from tax returns filed by taxpayers. They are notified of such collection by the Privacy Act Notice in the tax return instructions.

*Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?*

No

*Why not?*

Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations say that you must file a return or statement with us for any tax you are liable for. Your response is mandatory under these sections. Code section 6109 re-quires taxpayers to provide their identifying number on the return.

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

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant 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*

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Only

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

The IRS uses the On-Line 5081 (OL5081) to support the management of ELEC MFTRA accounts. When a user submits an OL5081 to gain access to the application, the Disclosure Manager receives a copy of the request via e-mail and can approve or deny access.

## 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.*

EMFTRA data is approved for deletion when no longer needed for operational purposes (NARA Job No. N1-58-09-93). These disposition instructions, as well as those for EMFTRA inputs, outputs and system documentation are published in IRS Records Control Schedule (RCS) Document 12990 under RCS 19 for Enterprise Computing Center-Martinsburg (ECC-MCC), item 76.

## SA&A OR ASCA

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

No

*Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?*

No

*Describe the system's audit trail.*

Windows event logs are collected on the folder containing the transcript data. The logs contain time/date stamp, user account, access type (read and write).

## 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)?*

Memorandum of Understanding with California Franchise Tax Board - 11/24/2004 Electronic MFTRA-LF767 Overview.vsd - (Demonstrates IRS Users-Disclosure have Read/Write in order to review and redact the file prior to release to CFTB) IRS-ELEC MFTRA-7511-CA-07-25-2011-1.pdf - Last ATO signed 07-24-2011 Email CR Approved for ELEC MFTRA.txt - Approval to remove ELEC MFTRA from the Federal Information Security Management Act (FISMA) Reportable Library - 04-02-2012 Master Inventory Change Request - ELEC MFTRA 3_20_2012.doc - Request to remove ELEC MFTRA from the FISMA Reportable Library 03-20-2012 Mod 8 Applications Development Transmittal Checklist - 17TCC-0420-U.pdf - 06-07-2017 Testing Checklist - 17TCC-0420-U.doc - 06-07-2017.

*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?*

Prior to being placed on the Remittance Transaction Research (RTR) production servers a process is in place to develop, test and document the results of the proposed changes. This includes a testing checklist to document the development and test process. As there is no complete set of test data that will test every condition, developers make every effort to perform unit testing and document the results which are placed in DocIT. If an issue is reported by a user on the Knowledge Incident Service Asset Management (KISAM) system, it is documented, and the mitigation is created by the developer and transmitted to production according to established procedures. If a security related change is required, the RTR developers will incorporate additional security test cases into the RTR Test Plan. In the event that changes will be made to the security posture of RTR, the RTR developers will conduct self-testing on the proposed changes, and the results, along with the date, will be subsequently documented and stored in DocIT. Additionally, user testing, as well as tests to determine the impact to security, are also performed, all of which are then presented to the CCB overseeing RTR application for final disposition. RTR is in compliance with IRM Section 10.8.6 for Secure Application Development.

## 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?*

Yes

*Explain the First Amendment information being collected and how it is used.*

Tax return data with IRS Criminal Investigation freeze codes redacted used for tax administration.

*Please list all exceptions (any one of which allows the maintenance of such information) that apply:*

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17).

The information maintained is pertinent to and within the scope of an authorized law enforcement activity (as noted in Q 7).

There is a statute that expressly authorizes its collection (identified in Q6).

*Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?*

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?*

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