Date of Approval: **November 10, 2020**

PIA ID Number: **5524**

SYSTEM DESCRIPTION

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

Lead Management - Fraud Referral & Evaluation, FRE

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?

Lead Management - Fraud Referral & Evaluation, #2891, Operation & Maintenance

What is the approval date of the most recent PCLIA?

10/11/2017

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.

Wage and Investment Division Risk Committee (W&I RC)

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 Lead Management - Fraud Referral & Evaluation (FRE) Program is part of Return Integrity & Compliance Services (RICS) under the purview of the Director of the RICS, Wage and Investment (W&I). The FRE Program missions are to detect new fraud leads and protect revenue; evaluate leads from external sources to determine future revenue protection potential; and provide analytical support to Return Integrity Verification Operations (RIVO) and other RIVO Departments. The FRE Program receives leads from: Industries, Banks, Preparers, Others (not incorporated into any of the other Program area), Security Breaches, State Taxing Agencies, Efile PIN, and Transcript. The FRE application will be used to house all internal/external leads that are received within FRE; assign and track these leads as they are worked; assist in cross-lead pattern analysis; and to provide FRE with more comprehensive reporting capabilities. RICS work is part of an overall revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. The sharing of leads between the IRS and the third-party entities are documented mutual arrangements, within IRC 6103 federal-state information sharing provisions, but not under a Memo of Understanding (MOU).

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

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

The SSN is only field that uniquely identifies the account. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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 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 FRE system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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

Standard Employee Identifier (SEID)

Internet Protocol Address (IP 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.

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?

Yes

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

IRS Employee Information: SEID, Employee IDRS ID Number, Taxpayer's Name Control, Notes Field (May Contain Additional Taxpayer Information). Additional Sensitive But Unclassified (SBU)/Personally Identifiable Information (PII): Preparer: address, Electronic Filing Identification Number (EFIN), Federal Submission ID, Preparer tax identification number (PTIN), Pattern Description. State: address, Submission ID, Device ID, Source Device ID, IPV4 or IPV6 Address, TCPort Number, Federal Submission ID, Foreign Address, Pattern Description, Transmission Info ID, IP Address, Source IP Address 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.

Return Integrity and Compliance Services (RICS) work is part of an overall IRS revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. The FRE application is required to maintain SSNs in the database from the third-party types of lead cases it manages in order to have the ability to research the leads to detect and prevent improper federal tax refunds. Industry Lead Personally Identifiable Information (PII) from software companies are related to suspicious tax return groupings that our industry partners have identified after return submission.

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

The PII information maintained in the FRE database is provided directly from third party sources. Input of the data received is entered either manually or automated into the FRE database. Assignment of FRE cases to tax examiners is manually entered by managers/administrators. Accuracy and completeness of data is inherited from the third-party sources to research cases provided.

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 42.021   Compliance Programs and Projects Files

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: Electronic Products & Services Support (EPSS)/FIRE
Current PCLIA: Yes
Approval Date: 11/16/2017
SA&A: Yes
ATO/IATO Date: 1/31/2018

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)?

Yes

For each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Various State Taxing Agencies
Transmission Method: Manual via industry fraud mailbox
ISA/MOU: No

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: American Coalition of Taxpayer Rights (ACTR)
Transmission Method: Manual via IVO FRE mailbox
ISA/MOU: No

Organization Name: Bank Leads
Transmission Method: Manual via IVO FRE mailbox
ISA/MOU: No

Organization Name: RPO-Complaints Referrals Group
Transmission Method: Manual via IVO FRE mailbox
ISA/MOU: No

Organization Name: Security Incident Reports from Software Providers
Transmission Method: Manual via IVO FRE mailbox
ISA/MOU: No

Organization Name: Software Company Industry Leads
Transmission Method: Manual via IVO FRE mailbox
ISA/MOU: 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: Dependent Data Base (DDb)
> Current PCLIA: Yes
> Approval Date: 6/17/2020
> SA&A: No
>
> System Name: Criminal Investigation (CI) Headquarters (HQ)
> Current PCLIA: Yes
> Approval Date: 4/6/2020
> SA&A: Yes
> ATO/IATO Date: 5/29/2020
>
> System Name: Return Review Program (RRP)
> Current PCLIA: Yes
> Approval Date: 12/6/2019
> SA&A: No

Identify the authority.

> Internal Revenue Code Sections 6001, 6011, 6012e(a) for federal tax administration

For what purpose?

> The FRE database is primarily utilized by employees of Return Integrity and Compliance Services (RICS)/Return Integrity Verification Operations (RIVO) as an inventory system to track cases from various third-party sources. The database provides an inventory management system in which cases are tracked from Tax Examiner (TE) assignment to closeout, maintaining a clear history of their existence. Criminal Investigation Headquarters (CI HQ) extracts data via SQL Reporting Service (SSRS) for further details on potential criminal cases. For the Return Review Program (RRP) and the Dependent Database (DDb), a weekly file of identified high risk taxpayer identification numbers (TIN) is provided via a RICS share where those files are picked up by these two programs.

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 IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code (IRC) sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

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

No

Why not?

The legal right to ask for information is IRC sections 6001, 6011, and 6012(a), and their regulations. They say that you must file a return or statement with IRS for any tax you are liable for. Your response is mandatory under these sections. Code section 6109 requires you to provide your identifying number on the return.

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

The program 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 Write

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

In order to obtain access to the FRE database, all prospective users must adhere to the RICS permissions portal process and 5081 process. The permission portal is used for controlling access, managing (create, modify, disable, delete) user accounts, and providing administrative rights to users. All requests are handled by the RICS Administrators and stored for auditing purposes. Additionally, all users are authenticated against the Active Directory validating their Standard Employee Identifier Number (SEID). All access requests must be authorized by the user's manager based on a user's position and need-to-know basis. Then the request must be approved at the FRE administrator level as well. All application administrator access requests must be authorized by the user's manager as well as an FRE administrator and system administrator. All approved database accounts will be logged. Access permissions are automatically configured to the database server after all approvals are received.

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?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

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?

Yes

Describe the system's audit trail.

FRE was developed by a vendor and the system audit trails have been put in place by the vendor. We have specified in the requirements for the project that an audit trail is mandatory and will contain all the audit trail elements as required by Internal Revenue Manual. Events tracked include - user and manager logon (date, time, SEID, action taken (add, update, delete)), user last accessed (date and time), source file uploads (date and time), appropriate user level access, authentication of user SEID upon logon against Active Directory, and removal of access due to 120 days inactivity (date). FRE is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

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)?

All test results are stored in RICS project management software. RICS .NET and Microsoft Access applications have a development (Dev) environment which is used for development and testing activities. This environment does not contain any PII data. All development and testing efforts are completed using simulated data. The development process involves developers releasing new functionality, enhancements, and defect fixes to the development environment. Each release is reviewed by the quality assurance team to ensure that both the business and technical requirements are met. All business requirement verification, functional testing, regression testing, and Section 508 testing is completed in the (Dev) environment. Issues found are remedied and subsequently released to the (Dev) environment for further testing and verification. All defects are tracked via project management software where team members can track the defects from opening to closure. The quality assurance team uses automated test scripts for regression and load testing on a secure intranet testing site for the (Dev) environment to further identify defects and verify against previous builds. Once defects are remedied, the latest code is released to the development environment. Once development is completed, User Acceptability Testing (UAT) is conducted. Upon completion of UAT, the application is released into Production Environment. The quality assurance team conducts preliminary testing in the Production environment to make sure the release meets the desired results and upon confirmation the application users are notified of the new release.

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 PII maintained in the FRE database is provided by internal IRS and external third-party sources. Accuracy and completeness of data is inherited from the internal and external sources.

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: Under 50,000

Contractors: Under 5,000

Members of the Public: 100,000 to 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