Date of Approval: 10/02/2025
Questionnaire Number: 2429

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Fraud Information Tracking System

Acronym:

FITS

Business Unit

Small Business and Self Employed

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The Fraud Information Tracking System (FITS) is a web-based database that allows monitoring, tracking, and controlling of potential fraud cases, both criminal and civil, by Office of Fraud Enforcement (OFE) personnel. Access to the system (and a user's respective role within the system) is controlled by a BEARS entitlement and/or authorization by IT. This system is owned and operated by OFE with technical support from IT. All OFE personnel could be users of the system whether it be the field office who interact directly with compliance employees in developing fraud cases or the policy office/business intelligence team in making data-driven decisions on the direction of OFE. This system is needed to benefit the IRS in the allocation of resources to identify and develop fraud cases across the Service. With OFE being a Servicewide support function, fraud cases can come from compliance employees in all operating

divisions (e.g. Taxpayer Services, SB/SE, BSA, LB&I, and TE/GE). FITS allows for Fraud Enforcement Advisors (FEAs) to document the actions taken to develop fraud cases which may result in civil fraud penalties and/or criminal referrals. Tracking the source and disposition of these cases allows for the monitoring of trends in fraud cases which are reported to business unit executives. The executives rely on this reporting to develop their ongoing fraud strategies. This tracking of fraud cases would also serve as one mechanism to respond to internal and external inquiries on the effectiveness of the IRS's fraud detection and prevention measures.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

FITS is not the originating/primary system where sensitive data is stored. The cases that ultimately enter FITS would have gone through the traditional case assignment process within SB/SE (examination and collection), Taxpayer Services, BSA, LB&I, and TE/GE. Systems used by those operating divisions serve as the primary location for sensitive data storage. When cases enter fraud development status, sensitive data for the respective case is transcribed on a form (Form 11661 or 11661-A, for example). The data is then copied from those fraud development forms into FITS. An activity record is maintained within FITS for all actions taken to develop a case for fraud. Various internal and external files can also be uploaded to FITS to support civil fraud penalties and/or a criminal referral. The cases within FITS have different "recommendations" applied which would systematically place a case into a different status. For example, when a Fraud Enforcement Advisor's involvement is complete, the case would no longer appear in FITS active inventory.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Citizenship or Migration Status
Comments (Social Media)
Credit Card Number
Criminal Record
Driver's License Number
Education Information
Email Address

Employer Identification Number
Employment Information
Family Members
Federal Tax Information (FTI)
Financial Account Number
Geographical Indicators
Individual Taxpayer Identification Number (ITIN)
Language
Medical History/Information
Name
Online Identifiers
Preparer Taxpayer Identification Number (PTIN)
Professional License Number
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers
Vehicle Identification Number (VIN)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII about individuals for Bank Secrecy Act compliance - 31 USC
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?
No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?
System

3 What Tier designation has been applied to your system? (Number)
2

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
No

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

This new submission is a result of some inquiries during a Government Accountability Office (GAO) audit.

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

SB/SE Governance

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

This system is associated with ABA#210592.

10 If this system discloses any PII to any third party outside the IRS, 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?

Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

No

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

Fraud Enforcement Advisors (FEAs) would be granted a user role where they have access to all taxpayer PII data for cases where they are supporting fraud development. An FEA manager would have access to all their FEAs' inventory, but which is limited to taxpayer names and a control number assigned by FITS. This access would allow for them to move a case to a different status within their group's inventory. A FITS administrator would have access to all control numbers and taxpayer names and can move cases between FEAs. A Superuser would have access to all PII within FITS and can make detailed changes to cases.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

A Privacy Act Statement is not used, and individuals are not given the opportunity to consent to the collection of their PII.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Under 50,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Under 100,000

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

Users of FITS go through the BEARS entitlement process to get access to their respective role. IT is the only party that can change a user's role after they are established.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

As cases are created and different recommendations are made to change the status of the case, an entry is recorded in the case history for each respective case. FITS reports can be run through Business Objects Environment (BOE) for various metrics recorded in the FITS interface. Audit trail logs are not sent to Splunk.

27 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Correspondence Examination Automation Support (CEAS), Issue Management System (IMS)

Incoming/Outgoing

Both

Transfer Method

Secure email/Zixmail

Interface Type

IRS Systems, file, or database

Agency Name

Integrated Collection System (ICS) and Business Objects Environment (BOE)

Incoming/Outgoing

Both

Transfer Method

Secure email/Zixmail

Interface Type

IRS Systems, file, or database

Agency Name

Integrated Data Retrieval System (IDRS), Report Generation Software (RGS)

Incoming/Outgoing

Both

Transfer Method

Secure email/Zixmail

Interface Type
Forms
Agency Name
Form 11661, Form 11661-A, Form 2797, Form 13549, Form 15521, and Form 13639
Incoming/Outgoing
Both
Transfer Method
Secure email/Zixmail

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
This SORN tracks and monitors employee access to IRS information systems containing taxpayer data. It helps to detect and deter unauthorized access to electronic records and prevent the misuse of taxpayer information. It ensures only authorized employees process or research work.

SORN Number & Name
IRS 37.006 - Correspondence, Miscellaneous Records, and Information Management Records
Describe the IRS use and relevance of this SORN.
FITS isn't the main system of records but rather stores miscellaneous records and correspondence for cases that enter fraud development status. These same records would be maintained on systems accessed by the compliance personnel.

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
GENERAL RECORDS SCHEDULE 4.2: Information Access and Protection Records
What is the GRS/RCS Item Number?
140
What type of Records is this for?
Electronic

Please provide a brief description of the chosen GRS or RCS item.

This schedule covers records created during agencies (1) responding to requests for access to Government information and (2) protecting information that is classified or controlled unclassified or contains personal data that is required by law to be protected.

What is the disposition schedule?

Varies - depends on when the business use ceases.

Data Locations

What type of site is this?

System

What is the name of the System?

Fraud Information Tracking System (FITS)

What is the sensitivity of the System?

Federal Tax Information (FTI)

What is the URL of the item, if applicable?

XXXXX

Please provide a brief description of the System.

See Executive Summary.

What are the incoming connections to this System?

Authorized users connect through the website identified above to manage their inventory of cases or perform administrative duties related to reporting.

What are the outgoing connections from this System?

Based upon the authorized user's selections of their assigned inventory, case histories and uploaded files are displayed.