Date of Approval: **April 05, 2022**

PIA ID Number: **6864**

SYSTEM DESCRIPTION

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

Flat File Data Dashboards, FFDD

Is this a new system?

Yes

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

Research, Applied Analytics and Statistics Internal Management

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Domain Architecture/Milestone 2

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

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.

To identify potential leads for criminal investigation, Research, Applied Analytics & Statistics (RAAS) conducts data analytics at the direction of IRS-Criminal Investigation, using data from the Compliance Data Warehouse (CDW). Data are analyzed and the results are transmitted via secure messaging and with file encryption in flat files in Excel format. The flat files contain charts and/or graphs to summarize the data presented in tabular form.

Flat file data dashboards in Excel format are used to identify leads for potential criminal investigations. The leads are vetted through IRS-CI's Nationally Coordinated Investigations Unit (NCIU), where further research is conducted, and the leads are evaluated for potential criminal investigation.

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:

Law enforcement and intelligence purposes

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

Taxpayer Identification Numbers are used in conjunction with other data to identify leads for potential criminal investigations.

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. Accordingly, Taxpayer Identification Numbers are used only when other unique identifiers are not available.

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
Place of Birth
Internet Protocol Address (IP Address)
Criminal History
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Financial Account Numbers
Employment Information
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.

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.

Proprietary data Business information that does not belong to the IRS.

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

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.

Virtual currency transaction identifiers and public virtual currency addresses.

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

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.

Social Security Numbers, Individual Taxpayer Identification Numbers and Employer Identification Numbers are the unique identifiers of leads for potential criminal investigation. These data, in conjunction with other indicators of tax non-compliance, are required to identify the individuals who perpetrate potential schemes for criminal investigations.

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

Research methodology first addresses data quality issues and uses corroborating information to validate the accurate, completeness and timeliness of data used in analytics supporting IRS-Criminal Investigation.

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 22.054 Subsidiary Accounting Files

IRS 22.060 Automated Non-Master File

IRS 22.062 Electronic Filing Records

IRS 24.046 Customer Account Data Engine Business Master File

IRS 26.020 Taxpayer Delinquency Investigation Files

IRS 34.037 Audit Trail and Security Records

IRS 42.008 Audit Information Management System

IRS 42.021 Compliance Programs and Projects Files

IRS 46.002 Criminal Investigation Management Information System and Case Files

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: Compliance Data Warehouse
Current PCLIA: Yes
Approval Date: 9/16/2020
SA&A: Yes
ATO/IATO Date: 5/29/2018

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: STATES SYSTEM
Transmission Method: Electronic
ISA/MOU: 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: IRS-Criminal Investigation
Current PCLIA: No
SA&A: No

Identify the authority.

IRS-Criminal Investigation is authorized to identify and investigate potential criminal activity related to tax administration.

For what purpose?

Flat files in Excel format are sent to IRS-Criminal Investigation. Flat files are not a database, and no Security Assessment and Authorization is required.

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?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Advance notification prior to detecting potential criminal activity would alert bad actors and imperil any subsequent criminal investigation.

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

No

Why not?

The data are used to detect illegal activity and other non-compliance.

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

Due process is addressed throughout criminal investigation and prosecution where applicable and when leads are selected for criminal investigation.

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 Contractor Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Only

Managers: Read Only

IRS Contractor Employees

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Administrator

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

Access to sensitive data is on a need-to-know basis determined by the analytics needs of the IRS-Criminal Investigation Nationally Coordinated Investigations Unit (NCIU). When flat files are transmitted to IRS-Criminal Investigation, two means of encryption are used. First, any file attachment is sent via encrypted email. Second, any file containing PII, or other sensitive information is password protected. The password is then transmitted to IRS-Criminal Investigation in a separate communication. Passwords and the files they control are never transmitted together.

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.

The longer of 10 years or the completion of any criminal investigation and prosecution. RCS 27 Item 54-Compliance Data Warehouse (CDW). The Compliance Data Warehouse (CDW) provides access to a wide variety of tax return, enforcement, compliance, and other data to support the query and analysis needs of the Research community. CDW provides a range of solutions to users, including data integration, computing services, data transfer, and educational services. CDW captures data from multiple production systems, migrating the data to the CDW environment, transforming, standardizing, and augmenting the data, and organizing the data In a way that is conducive to analysis A. Inputs: The Compliance Data Warehouse (CDW) receives inputs from the Audit Information Management System (AIMS), Automated Under-reporter AUR), Accounts Receivable Dollar Inventory (ARDI), Business Master File (BMF), Business Returns Transaction File (BRTF), Exam Operational Automation Database (EOAD), Enforcement Revenue Information System (ERIS), Individual Master File (IMF), Individual Returns Transaction File (IRTF), Information Returns Master File (IRMF), and the National Research Program (NRP). (GRS 4.3, Item 020, Job No. DAA-GRS-2013-0001-0004) AUTHORIZED DISPOSITION Delete/Destroy any cached input files and data immediately following validation of receipt by the system. B. System Data: Contents of the Compliance Data Warehouse (CDW) consist of information on taxpayers, tax preparers, financial institutions, or legal entities (e.g., Power of Attorney), and various tax return characteristics. (Job No. N1-58-10-7) AUTHORIZED DISPOSITION Cut off at end of the Processing Year. Delete/Destroy 10 years after processing year, or when no longer needed for operational purposes, whichever Is later. C. Outputs: Outputs from the Compliance Data Warehouse (CDW) consist of archived database updates, which occur on a monthly, quarterly, and annual basis. Research analysts query and analyze these data to produce reports, tables, and other statistical information. (GRS 4.3, Item 031, Job No. DAA-GRS-2013-0001-0006) AUTHORIZED DISPOSITION Delete/Destroy 10 years after data update, or when no longer needed for operational purposes, whichever is later. D. System Documentation: System documentation consists of codebooks, records layout, user guides, and other related materials. (GRS 3.1, Item 051, Job No. DAA-GRS2013-0005-0003) AUTHORIZED DISPOSITION Delete/Destroy when superseded or 5 years after the system is terminated, whichever is sooner.

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.

All requests for data and analytics from the IRS-Criminal Investigation Nationally Coordinated Investigations Unit are approved by CI Management. The Compliance Data Warehouse has access auditing and monitoring security features.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

The data visualizations and analytics are familiar to the IRS Employees involved and to the contractor team, and the processes are straightforward. No testing is required prior to implementation.

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?

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.

Analytics have the potential to identify collusion among individuals engaged in tax non-compliance or other financial schemes. Since the data for analysis are from the Compliance Data Warehouse, auditing/logging controls are in place for data use.

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