Date of Approval: **May 01, 2020**

PIA ID Number: **4879**

## SYSTEM DESCRIPTION

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

Selection aNd Analytic Platform, SNAP

*Is this a new system?*

Yes

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

Strategic Development (SD)

*Current ELC (Enterprise Life Cycle) Milestones:*

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.*

Selection aNd Analytic Platform (SNAP) is a Federal Risk and Authorization Management Program (FedRAMP) approved cloud-based platform that will replace the current Return Review Program (RRP) database querying functionality related to the Electronic Fraud Detection System (EFDS). The new platform will continue to allow business users from Criminal Investigations (CI) and Wage and Investment (W&I) to perform critical ad-hoc searches and manual research used for revenue protection to help identify fraud, quality assurance to identify returns not authenticated as identify theft and to allow reporting on tax returns, scheme development to analyze data sets and fraud trends, and support new and ongoing investigations. Selection aNd Analytics Platform (SNAP) and the Palantir Federal Cloud Solution (PFCS) will be implemented to replace all current Electronic Fraud Detection Systems (also known as Return Review Program Legacy Component (RRP LC) Oracle DISCOVERER functionality. Discoverer is a critical ad-hoc querying and manual research tool used by Business users from Criminal Investigation (CI) and Wage and Investment

(W&I) for the following business processes: Revenue Protection - perform research to identify fraud not identified by models, filters, or rule breaks, process leads to identify associated tax returns, and manually identify Identity Theft (IDT) cases. Quality Assurance - query data to identify returns authenticated as not IDT, conduct research to identify inventory for civil treatment streams, and conduct executive reporting. Scheme Development - research and analyze large data sets to identify the full scope of investigations and identify emerging fraud trends. Support Investigations - research and analyze large data sets to identify full scope of new/ongoing civil criminal investigations, and support field agents and investigators with time sensitive data and requests. The research is not generated by artificial intelligent machine learning and SNAP conducts focused investigations and does not perform expansive data mining. SNAP does not use Artificial Intelligence Supervised or Non-Supervised Learning.

## 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:*

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Delivery of governmental benefits, privileges, and services

Another compelling reason for collecting the SSN

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

The Social Security Numbers (SSN) is the primary means of updating or querying the data by other internal systems. It is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct records are accessed by IRS systems or when research is done on fraud cases. In addition, the SSN is used to restrict access by complying with the Taxpayer Browsing Protections Act.

*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 (OMB) circular-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 SSN is the significant part of the data being processed/received/disseminated by SNAP.

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

Internet Protocol Address (IP Address)

Financial Account Numbers

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

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.*

Document Locator Number (DLN), Income; Withholding; and Deduction information (Individual Master File/Business Master File), Tax Refund Amount, Type of Tax Return Filed, Source of Tax Return Filing (Paper or Electronic), Tax Filing Status, Number of Dependents, Name of Dependents, Employer Name, Employer Tax Identification Number, Employer Address, Employer Telephone Number, Bank Account Information, Date of Death, Device Identification, Prison/Prisoner Information, Electronic Filing Identification Number (EFIN), Preparer Tax Identification Number (PTIN), Tax Return Preparer Name and Employer Identification Number (EIN).

*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.*

SNAP receives SBU/PII data from the RRP application that receives SBU/PII data from multiple internal IRS systems. This data is used strictly for related business needs that focuses on improving the prevention of lost revenue associated with fraudulent tax returns through better detection of fraudulent activities. This includes the SSN since it is the one unique identifier for taxpayers that is common across internal IRS systems and is used to research questionable activities related to fraudulent returns. In addition, it is being used as part of an enterprise solution related to the access restrictions to ensure compliance with IRS policy and federal requirements. NOTE: The system also functions in training mode, where all of the data available in production is available for training. Only those users authorized to access the system in production are authorized to access it for training, with the same OnLine5081 process and other access controls in place. The training data remains within the secure IRS environment.

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

SNAP will receive daily control file updates containing updated data from RRP. Upon receiving the data files, a series of data health and integrity checks (e.g. checksum comparison, confirming row counts, etc.) occur to ensure that all expected data is present. Once all files are processed, an acknowledgement file is automatically generated and returned. If any discrepancies are found, RRP will resend the required data files.

## 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 46.002 | Criminal Investigation Management Information System and Case Files |
| IRS 42.021 | Compliance Programs and Projects 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: Return Review Program (RRP)
Current PCLIA: Yes
Approval Date: 10/6/2017
SA&A: Yes
ATO/IATO Date: 4/17/2019

*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: Electronic Fraud Detection System (EFDS)
Current PCLIA: Yes
Approval Date: 1/10/2018
SA&A: Yes
ATO/IATO Date: 5/9/2019

System Name: Return Review Program (RRP)
Current PCLIA: Yes
Approval Date: 10/6/2017
SA&A: Yes
ATO/IATO Date: 4/17/2019

*Identify the authority*

Internal Revenue Code Section 6109 authorizes the collection and use of SSN information.

*For what purpose?*

Purposes for collecting, processing, and disseminating information to IRS systems is for the purposes of tax administration along with detecting and preventing both identity theft and fraudulent tax refunds as authorized under Internal Revenue Code Sections 6001, 6011, 6012e(a).

*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?*

Yes

*Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?*

Yes

*Date Certified*

12/4/2019

*Please identify the ownership of the CSP data.*

IRS

*Does the CSP allow auditing?*

Yes

*Who audits the CSP Data?*

3rd Party

*What is the background check level required for CSP?*

Moderate

*Is there a breach/incident plan on file?*

Yes

*Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:*

Storage

Transmission

Maintenance

*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?*

Data is received from other IRS sources/systems that directly interacts with the taxpayer prior (upstream) to data collection. Those other sources/systems provide the Privacy Act Notice to individuals at the time of collection. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

No

*Why not?*

Data is received from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals at the time of collection providing the opportunity to decline or consent. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

Data is received from other IRS upstream sources/systems and SNAP does not interact with taxpayers directly and thus "due process" is addressed by other IRS applications/interactions that directly interact with taxpayers. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any others ensuing actions will directly interact with taxpayers. Thus, due process is awarded during any ensuing criminal investigation or civil action. Due process is provided pursuant to 26 USC and 18 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 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 System Administrators: Read Write

Contractor Developers: Read Write

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

The users must submit an OL5081 to request access to the SNAP application. The request must be approved by the user's manager before being forwarded to the SNAP Business Units (BU). The SNAP users BUs are responsible for reviewing the request and ensuring the users are added to the appropriate access control list for the user to receive proper access to the SNAP data. Before access is granted, the user is required to digitally sign OL5081 acknowledging his/her security responsibilities when using the system. The user signs security rules of behavior provided in the OL5081. Pursuant to the rules described in UNAX (Unauthorized Access of Taxpayer Accounts), employees are not allowed to access their own accounts, their spouses account and immediate family member's account. Third-party providers (i.e., contractors) for the SNAP application are subjected to the same application system policies and procedures of the IRS as employees. Additionally, contractors must conform to the same security controls and documentation requirements that would apply to the organization's internal systems; which are enforced through the appropriate Contracting Officer's Representative (COR). IRS and contractor employees must successfully pass Personnel Screening and Investigation, (PS&I) appropriate to their need and be trained on Internal Revenue Service (IRS) security and privacy policies and procedures, including the consequences for violations. SNAP Developers will have read and write access to data in order to support the construction and maintenance of production data pipelines. No direct edits to the data pipeline logic or code will be allowed on the Production master branch of the system. All pipeline maintenance will be implemented and tested on a staging branch before changes are merged into the production pipeline. In order to support the process of merging changes into production data pipelines, developers need read/write access to production data. All developer access to data is logged in the same manner as any other user, and those logs are sent to ESAT Enterprise Security Audit Trails from Palantir in various formats for analysis.

## 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.*

SNAP records owners and developers are working with the IRS Records Office to draft data retention requirements for submission to/approval by the National Archives and Records Administration (NARA). Proposed minimum business need for the data is four years (current year, plus three prior processing years). All records managed in SNAP will be erased or purged from the system in accordance with approved retention periods. RCS 32 Item 50 Return Review Program. Return Review Program (RRP). RRP is used to electronically track, report, monitor, and assign processing of pre-refund tax returns to prevent criminal and civil noncompliance. A. Inputs: The RRP database and applications interface with other electronic data sources to receive taxpayer data and tax returns data required for scheme modeling, non-compliance research, and report generation (GRS 4.3, Item 020, Job No. DAAGRS- 2013-0001-0004). Those data sources include: MeF (Modernized e-File) Records- Data transfers from source systems to RRP vary from system to system, organization to organization. Source systems transfer data to RRP systems on a daily, weekly, monthly, and annual basis. Recordkeeping requirements for each of the RRP data sources are appropriately scheduled in the context of other IRS disposition authorities unique to those systems and/or sources providing input. B. System Data: RRP contains taxpayer (individual/business) entity and form information from various sources to support tax return anomaly detection analysis. All data is considered sensitive and is handled using Personally Identifiable Information (PII) procedures. (Job No. DAA-0058-2014-0002-0001)-AUTHORIZED DISPOSITION Cut off RRP data at the end of the calendar year. Retain RRP data in system data tables for 3 years after cutoff, then archive. Maintain RRP archived data until no longer needed. C. Outputs: RRP users can run ad hoc queries, create standard reports, and perform data analysis. Users can also schedule and run reports in batch mode and send the links for reports via email to another user. Users can save reports to a file location or in a personal folder in MS Excel, PDF, or CSV format. It is the user's responsibility to determine whether the report should be emailed to others following the IRM security and privacy guidelines and using IRS approved email tool. -AUTHORIZED DISPOSITION Destroy/Delete when no longer needed for legal, audit, or other operational purposes. D. System Documentation: Enterprise Life Cycle (ELC) Milestone documentation, system design schema, user guides/manuals. (GRS 3.1, Item 051, Job No. DAAGRS- 2013-0005-0003)-AUTHORIZED DISPOSITION Destroy/Delete 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.*

SNAP is authorized by the FedRAMP Security Threat Analysis Report (FSTAR). As a part of security oversight, and in support of Federal and IRS requirements, SNAP records and processes security events that are produced by the software and IT systems that make up the system. Most of the systems IT components generate events related to the systems, its usage, and query activities occurring on the system. Events may be collected from multiple sources, including, but not limited to this IRS system, this system's IRS IT support systems, this system's users, this system's software service provider, and this system's cloud service provider. The IT events are recorded in event logs and are typically collected, processed and stored according to Federal and IRS requirements. The event logs are captured in various formats and sent to ESAT for processing to determine the presence of events that may be relevant to the security posture of the system. Event logs may be aggregated and evaluated for patterns that may indicate information about the system's security posture and to recreate specific activities. Relevant security events may be considered actionable and may be used to indicate actions or changes that need to be made to the system to maintain or improve the security posture of the system or its components.

## 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)?*

Internal IRS SharePoint site

*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?*

SNAP is a component of the Discoverer Replacement Palantir Solution (DRPS) project and DRPS has a completed System Test Plan (STP). SNAP will complete subsequent test plans as needed when system enhancements are made. Each enhancement will have a different set of design requirements which includes both security and privacy requirements. The privacy requirements are based on the appropriate privacy principles.

## 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: 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?*

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