

Date of Approval: **May 16, 2023**

PIA ID Number: **7778**

SYSTEM DESCRIPTION

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

Return Order and Delivery System - Delivery Model, ROADS DM Automation

Is this a new system?

Yes

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

Data and Analytics Advisory Group (DAAG)

Current ELC (Enterprise Life Cycle) Milestones:

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 SB/SE Return Order and Delivery System (ROADS) Delivery Model (DM) is an intelligent automation solution used to deliver new exam cases to the appropriate groups based on the available inventory, capacity of groups, and priorities from Business Operating Division (BOD) exam plans. The automation leverages data from various reports that include information on targets to meet for the year, exam cases in progress, exam cases available for employees to work, and capacity of employees at PODs to take on new exam cases. The automation includes a front-end user interface developed using R Shiny that allows users to upload data files, run a back-end optimization model developed in Python, and review and download outputs on the web-based user interface or as an excel file. This process will save users time, modernizes the current technology infrastructure of the system, and provides net-new features.

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

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

The report of available cases uploaded into the ROADS DM Automation contains SSN information. SSNs are used to identify new exam cases and needs to process the information to be able to deliver the appropriate exam cases to the appropriate groups to be worked based on various constraints. The use of SSNs is permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their tax returns.

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

We will not be storing any SSNs or PII. We will require a user to have the appropriate access to the application. The application does not provide any additional PII data that the user already has access to in the existing reports. 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.

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

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.

Are there other types of SBU/PII used in the system?

No

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 for personnel administration is 5 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.

The ROADS DM Automation requires various data input files to process which new exam cases need to be delivered to which groups, dependent upon geographic and capacity constraints. The need for SSNs and PII is to identify exactly which exam cases should be delivered to ensure the best cases are prioritized. There are checks in place to ensure the analyzed outputs are only displayed to users with access. Outputs will not be returned if these credentials do not work. The tool also logs user activities in a SQLite database.

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

No alteration is done to the input data files received through the automation. The data is as accurate, complete, and timely as the data contained in input 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 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?

No

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?

No

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?

Yes

Identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Research, Applied Analytics and Statistics (RAAS) Contractors
Transmission Method: Secured Email
ISA/MOU: No

Identify the authority.

IRC 6103(n) Certain other persons Pursuant to regulations prescribed by the Secretary, returns and return information may be disclosed to any person, including any person described in section 7513(a), to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration.

For what purpose?

Yes

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

Yes

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?

Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC. Information is collected from existing IRS systems; some of which was submitted previously by the taxpayer. The system does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC. The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

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

The system does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines and 5 USC. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected.

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: Administrator

IRS Contractor Employees

Contractor Developers: Administrator

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

Access to the ROADS DM tool is requested via Business Entitlement Access Request System (BEARS). Data access is granted on a need-to-know basis. The BEARS enrollment process requires that an authorized manager approve access requests. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. Write, Modify, Delete, and/or Print are defined on BEARS and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. A request will need to be submitted for access to the ROADS DM tool. Management monitors system access and removes permissions when individuals no longer require 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.

The ROADS DM Automation audit and user logs are scheduled under General Records Schedule (GRS) 3.1 for General Technology Management Records, Item 020. IRS System Technology audit logs are maintained per IRM 5.1.25.6 in the Security Audit and Analysis System (SAAS) RCS 19 Item 88 Audit Logs will be erased or purged from the SAAS at the conclusion of their retention period(s) as required under IRM 1.15.6. The method used for sanitization will follow NIST SP 800-88 guidelines. These will not be stored in the ROADS DM Automation, but a SQLite data base.

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?

Do not know.

Describe the system's audit trail.

Limited scale local log-based auditing is in place and will be stored in SQLite database. The logging functionality of the ROADS DM tool will capture key events conducted by users. Each event will be associated with an individual user, session, timestamp, and additional metadata (e.g., tool version, event type).

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

The automation is reviewed by the Administrators to verify the automation performs the same activities as the current Subject Matter Expert (SME). Code reviews and document reviews are also conducted to ensure the application performs as expected. Appropriate BEARS access is needed for access to the ROADS DM automation prior to allowing users to use the tool. The ROADS DM tool logs key user interactions with the tool in a SQLite Database on the deployment server.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

No

Explain why not:

We are testing locally and have the appropriate permissions to view reports containing SBU data. The application displays information but does not save the information, therefore any SBU data is not stored in testing, and is only visible to the user that has appropriate permissions to access this sort of data. The automation is reviewed by the administrators to verify the automation performs the same activities as the current SME. Code reviews and document reviews are also conducted to ensure the application performs as expected. Appropriate BEARS access is needed for access to the ROADS DM automation prior to allowing users to use the tool and conduct analyses. The ROADS DM tool logs key user interactions with the tool in a SQLite Database on the deployment server.

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

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