Date of Approval: **September 22, 2023**

PIA ID Number: **7795**

SYSTEM DESCRIPTION

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

Soft Letter Management and Reporting Tool, SMART

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?

International Individual Compliance-Organization, IIC Organization, Operations & Maintenance

What is the approval date of the most recent PCLIA?

7/1/2021

Changes that occurred to require this update:

Conversions

Significant System Management Changes

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.

M365 Technical Review Board

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 Smart Letter Management And Reporting Tool (SMART) is a collective repository of taxpayer mailed responses to IRS soft letters issued covering multiple campaigns within Large Business and International (LB&I) and other Business Units BU, Small Business and Self Employed (SBSE). Compliance Support, Development & Communication (CSDC) of LB&I receives taxpayer phone calls and mailed responses for these campaigns. SMART is a centralized source to input the taxpayer correspondence which may include taxpayer's name, taxpayer's identification number, taxpayer's address and for campaign owners such as LB&I tax analyst to analyze these. There are currently over 80,000 soft letters which contain taxpayer names, identification number, and address mailed by CSDC recorded in the SMART database. SMART architecture uses a connection between an M365 Power Platform dedicated environment and on-premises SQL database. Connecting by a Microsoft service account the tool has four M365 PowerApps forms to create and modify over twenty tables which contain taxpayer PII listed under section B PII detail in the database. SMART is at the core of the analysis and deep insights into connective compliance actions resulting from sending soft letters. SQL databases and the M365 dedicated environment create the ideal system allowing for practice area reporting as well as campaign specific reporting. Using data analytics, SMART allows teams to measure compliance activities, inform decision-making and improve operational outcomes of the campaign compliance program and treatment streams selection process.

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).

Tool incorporates external data sources containing SSNs. System acts as a repository for this external data source and matches LB&I treatment stream activities with data sources using SSNs.

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

SSNs will be masked to users of the system.

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
Internet Protocol Address (IP Address)
Financial Account Numbers

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.

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.

Taxpayer File Year and Power of Attorney information; Employee Name and Grade; examination selection and results; Audit Risking results; Offshore Compliance information from other federal agencies; Exchange of Information taxpayer data, from foreign tax administrations.

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

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.

PII/SBU information is required to properly identify taxpayers and accurately associate taxpayer information for monitoring and compliance purposes, including some information received from other federal agencies and via the exchange of information programs from foreign tax administrations. Taxpayer identity information (including name, SSN, address, and tax year) and employee Standard Employee Identifier (SEID) is required to properly identify, associate, and monitor CWAs, OTSA and ATP compliance work, and other international individual compliance cases. 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. International Individual Compliance (IIC) Teams, Foreign Payments Practice (FPP), CWA, Exchange of Information (EOI), Practice Network (PN), Offshore Compliance Initiatives (OCI), JITSIC and OTSA offices require the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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

The site owner is responsible for the accuracy, timeliness, and completeness of the information on the site. The site owner is the program manager and the lead for the specific program. The senior program analyst responsible for the statistical sampling inventory validation listing (SSIVL) reports is responsible for the content on the site. For the classifying and building of cases for potential examination, the Compliance and Data Analytics program manager is responsible for the content on the site. Access to add, delete, edit, update, or otherwise change information on the site is controlled and limited.

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 00.001 Correspondence Files and Correspondence Control Files

IRS 00.002 Correspondence Files: Inquiries about Enforcement Activities

IRS 42.001 Examination Administrative Files

IRS 42.031 Anti-Money Laundering/Bank Secrecy Act and Form 8300

IRS 34.037 Audit Trail and Security Records

IRS 49.001 Collateral and Information Requests System

IRS 22.027 Foreign Information System (FIS)

IRS 42.017 International Enforcement Program Information Files

IRS 49.002 Tax Treaty Information Management System

IRS 26.019 Taxpayer Delinquent Account Files

IRS 26.020 Taxpayer Delinquency Investigation Files

IRS 36.003 General Personnel and Payroll Records

IRS 00.001 Correspondence Files and Correspondence Control 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?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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.

10/17/2022

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

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?

Individuals are solicited by the Internal Revenue Service for specific information pertaining to large business and International campaign strategies. It is voluntary disclosure of the taxpayer to respond and transmit information pertaining to their tax behavior in regard to the campaign solicitation.

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):

Individuals are not mandated to respond to the solicited IRS letter.

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

Not Applicable

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

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

Controlled access is maintained through bears entitlement granted on a system management and employee management permission structure. Access to particular taxpayer information is controlled by management's employment assignment through SharePoint permissions to the related campaign under which the taxpayers listed in the system. Non-assigned employees are unable to access taxpayer information or edit the information if they do not have entitlement permissions or SharePoint permissions.

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.

PII/SBU information is electronic and is held as long as necessary until the specific case is closed (IRM 1.15.1.7.6) Aggregate program information, without specific taxpayer PII or SBU, from closed cases is maintained for about 4 years for operational measures and comparatives with other years or programs, and for organizational management. Documents stored in this site are not the official records and therefore the site is not considered an official recordkeeping system. The Site Owner will ensure that site documents are appropriately destroyed/deleted when no longer needed for reference. Official recordkeeping copies of LB&I records are maintained in accordance with Records Control Schedule (RCS) 26, items 1-53, published in RCS Document 12990.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

12/28/2021

Describe the system's audit trail.

The application's SQL database will have auditing turned on to allow tracking of data modifications. Those audits are stored in the server logs. The audit saved user SEID and date/time and database modification.

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)?

Test results are stored on the M365 Program Management Office 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?

Development testing and regression testing occur to include applicable privacy requirements being performed on the impacted M365 dedicated environment and the SQL database. These include but are not limited to access control testing, authorization process testing, and PII masking validation.

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: 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