Date of Approval: **October 28, 2020**

PIA ID Number: **5620**

## SYSTEM DESCRIPTION

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

System 7.5 - IT Operational Reporting, Sys 7.5, System 7.5 - ITOR

*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?*

System 7.5 - IT Operational Reporting, Sys 7.5 - ITOR, # 3083

*What is the approval date of the most recent PCLIA?*

12/18/2017

*Changes that occurred to require this update:*

Expiring PCLIA

*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.*

Application Development (AD) Data Delivery Services (DDS) Governance Board (GB)-AD:DDS:GB

*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.*

In the early phases of the Affordable Care Act (ACA) implementation, Treasury Inspector General for Tax Administration (TIGTA) auditors determined there was no visibility into the health and performance of ACA systems and technologies. This created a business need to establish the Information Technology Operational Reporting (ITOR) Data Mart, which collects and electronically stores performance and information about ACA technology systems. These systems consist of hardware and software components and enable the collection, creation, storage, and distribution of ACA information electronically. The ACA systems work together to ensure that the IRS can intake and process taxpayer returns as required by the ACA legislation. The IRS uses information from ITOR to understand the health of these ACA systems, ensure adherence to performance standards, and identify any irregularities. ITOR gives critical visibility into the vast complexity of the IRS ACA systems. The information consists of 11 IT System data elements in a pre-determined format by the IRS Solutions Engineering operating division. As an example, ACA system stakeholders can use the information to ensure enough resources are allocated for taxpayer return processing, identify bottlenecks, and any system outages. To provide the most visibility into Information Returns processing to ITOR stakeholders, the ITOR environment intakes the Transmitter Control Code (TCC), which is considered Sensitive but Unclassified (SBU) information, from two IRS internal ACA systems (see below). The TCC is a unique 5-digit identification number assigned to external entities which submit information returns. It is considered a "low-risk" PII. It ultimately allows ITOR users to identify any issues with these submitters related to Information Returns processing. ACA Information Returns (AIR): This IRS system is responsible for accepting, processing, and storing health coverage data from insurance providers and other entities Integrated Enterprise Portals (IEP): This IRS system is the taxpayer online environment, and is the external facing system used to meet taxpayer demands for self-service tax-related needs. In October of 2020, the ACA ITOR Data Mart blueprint was leveraged to establish an ITOR Data mart and support operational metrics.

# 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.)?*

No

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?*

No

*Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?*

No

*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.*

Transmitter Control Code (TCC)

*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)

*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.*

As stated in section 5, the TCC identifies the external entity, which is the business operator who has submitted the Information Returns. Business users need this information in order to identify specific issues with Information Return transmissions, and follow-up with the specific sender of the Information Returns to address these issues if necessary.

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

The TCC information is verified for accuracy, timeliness, and completeness prior to receiving the information in the ITOR environment. Thus, ITOR performs no validation of this information, and further information about the verification of this element may be found in the PCLIA documents for Integrated Enterprise Portals (IEP) and ACA Information Returns (AIR).

## 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.*

No

## 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: ACA Information Returns (AIR)
Current PCLIA: Yes
Approval Date: 9/28/2020
SA&A: Yes
ATO/IATO Date: 3/14/2020

System Name: Integrated Enterprise Portal (IEP)
Current PCLIA: Yes
Approval Date: 11/22/2019
SA&A: Yes
ATO/IATO Date: 12/19/2019

*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: System 61 Business Analytics (BA)
Current PCLIA: Yes
Approval Date: 4/8/2020
SA&A: No

*Identify the authority.*

System 61 Business Analytics (BA), hosts the Business Object Enterprise (BOE) Reporting and Tableau visualization software. This was initially requested by Release Level Technical Support (RLTS), an IRS operating unit responsible for IT requirements, for ITOR to provide BOE reporting about TCC Information.

*For what purpose?*

Note that this BOE reporting is accessible only to IRS Employees for reporting purposes.

*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.*

The ITOR system does not collect any information outside of the IRS, third party sources, or from individuals directly. The ITOR information is only received from other systems within the IRS. Furthermore, information regarding how these non-ITOR ACA systems collect the information may be found in their corresponding Privacy Impact Assessment (PIA) documentation.

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

No

*Why not?*

ITOR receives its information directly from other ACA and PBBA systems within the IRS only and opportunities for individuals to decline from providing information are not applicable to the ITOR system. The ITOR system has no interaction or correspondence with individuals outside of the IRS.

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

Information is received from systems within the IRS, and corrections to the information will be handled by other ACA systems within the IRS. Access to the information is completed through Online 5081 (OL5081), which is an IRS internal system used to request access and approval to be able to use different technologies (i.e. Email, Internet Access, Software Access, etc.) within the IRS. Once users have received access through OL5081, they may either read, view, or edit the information depending on the level of access granted.

## 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 Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Only

*IRS Contractor Employees*

Contractor Users: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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

IRS management must approve all access to Sensitive But Unclassified (SBU) or Personally Identifiable Information (PII) for IRS employees and contractors through the OL5081 process. This request has to be approved by the potential user's manager based on a user's position and need-to-know.

## 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.*

All information housed in the ITOR system will be erased or removed from the system in accordance with approved period of information possession. It is the official storage unit for data and documents and has National Archives approval to affect how this information is stored or arranged. Any records generated and maintained by the system will be managed according to requirements under Internal Revenue Manual (IRM) 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedule (RCS) 19, Item 91, Job No. DAA-0058-2016-0009, approved 6/27/16; and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

## 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.*

The ITOR system's audit trail can be found in required documentation in accordance with ELC. ITOR ensures that all parts of the Software Development Lifecycle (SDLC) are documented properly on SharePoint and ReqPro for traceability back to the original IRS customer requests and requirements.

# 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 ISR-A&R 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?*

A series of tests are conducted to validate the system configuration. Data accuracy is not only a requirement of the IRS principles; it is part of the Privacy Act and Federal Taxpayer Information protection laws and regulations. In order to protect taxpayer information, the recommendation is to use sanitized data when possible in order to reduce the risk of PII being seen by individuals without a need-to-know and creating an incident. However, there are instances when using live data may be needed. The IRS has established IRM 10.8.8. The ITOR system has completed testing with BOE integration for the PII data folder and milestone exit review audit activities to ensure that the Privacy Requirements have been met.

## 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:*

Because the TCC is considered low-risk PII, it is by default also considered SBU information. Because information containing the TCC may be needed in the future for testing, the Form 14665 Data Use Questionnaire is required for both AIR and IEP, which are sources for this information. It has been concluded that AIR, IEP, and ITOR all operate on a Federal Information Processing Standard (FIPS) 199 Environment Classification of "moderate" and an SBU Data Use Request is not required. Formal acceptance of the questionnaire is pending approval.

*Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?*

## 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: Not Applicable

Other: Yes

*Identify the category of records and the number of corresponding records (to the nearest 10,000).*

More than 100 million records containing TCC.

## 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