

---

**A. SYSTEM DESCRIPTION**

---

1. Enter the full name and acronym for the system, project, application and/or database. System 7.5 - IT Operational Reporting, Sys 7.5 - ITOR

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

System 7.5 - IT Operational Reporting, ITOR , Sys 7.5 - ITOR, PIA 1516

Next, enter the **date** of the most recent PIA. 12/8/2015

Indicate which of the following changes occurred to require this update (check all that apply).

|     |  |
|-----|--|
| Yes | Addition of PII                                      |
| No  | Conversions  |
| No  | Anonymous to Non-Anonymous                           |
| No  | Significant System Management Changes                |
| No  | Significant Merging with Another System              |
| No  | New Access by IRS employees or Members of the Public |
| No  | Addition of Commercial Data / Sources                |
| No  | New Interagency Use                                  |
| No  | Internal Flow or Collection                          |

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

|     |  |
|-----|--|
| No  | Vision & Strategy/Milestone 0                                    |
| No  | Project Initiation/Milestone 1                                   |
| No  | Domain Architecture/Milestone 2                                  |
| No  | Preliminary Design/Milestone 3                                   |
| No  | Detailed Design/Milestone 4A                                     |
| No  | System Development/Milestone 4B                                  |
| No  | System Deployment/Milestone 5                                    |
| Yes | Operations & Maintenance (i.e., system is currently operational) |

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

---

**A.1 General Business Purpose**

---

5. 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 ITOR Data Mart, which collects and electronically stores performance and throughput 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.

---

## B. PII DETAIL

---

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Transmitter Control Code (TCC)

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)

No SSN for tax returns and return information is Internal Revenue Code Section 6109

No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

No PII for personnel administration is 5 USC

No PII about individuals for Bank Secrecy Act compliance 31 USC

No Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

---

**B.1 BUSINESS NEEDS AND ACCURACY**

---

7. 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 the 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.
8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. 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).

---

**C. PRIVACY ACT AND SYSTEM OF RECORDS**

---

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes
- 9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? No

---

**D. RESPONSIBLE PARTIES**

---

10. Identify the individuals for the following system roles. ## Official Use Only

---

**E. INCOMING PII INTERFACES**

---

11. Does the system receive SBU/PII from other system or agencies? Yes
- 11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

| <u>System Name</u>                 | <u>Current PIA?</u> | <u>PIA Approval Date</u> | <u>SA &amp; A?</u> | <u>Authorization Date</u> |
|------------------------------------|---------------------|--------------------------|--------------------|---------------------------|
| ACA Information Returns (AIR)      | Yes                 | 10/17/2016               | Yes                | 04/18/2017                |
| Integrated Enterprise Portal (IEP) | Yes                 | 12/07/2015               | Yes                | 04/04/2017                |

- 11b. Does the system receive SBU/PII from other federal agency or agencies? No

- 11c. Does the system receive SBU/PII from State or local agency (s)? No
- 11d. Does the system receive SBU/PII from other sources? No
- 11e. Does the system receive SBU/PII from **Taxpayer** forms? No
- 11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

---

## F. PII SENT TO EXTERNAL ORGANIZATIONS

---

12. Does this system disseminate SBU/PII? Yes
- 12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

| <u>System Name</u> | <u>Current PIA?</u> | <u>PIA Approval Date</u> | <u>SA &amp; A?</u> | <u>Authorization Date</u> |
|--------------------|---------------------|--------------------------|--------------------|---------------------------|
| System 61 BA       | Yes                 | 05/31/2017               | No                 |                           |

Identify the authority and for what purpose? 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. Note that this BOE reporting is accessible only to IRS Employees for reporting purposes.

- 12b. Does this system disseminate SBU/PII to other Federal agencies? No
- 12c. Does this system disseminate SBU/PII to State and local agencies? No
- 12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No
- 12e. Does this system disseminate SBU/PII to other Sources? No

---

## G. PRIVACY SENSITIVE TECHNOLOGY

---

13. Does this system use social media channels? No
14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No
15. Does the system use cloud computing? No
16. Does this system/application interact with the public? No

---

## H. INDIVIDUAL NOTICE AND CONSENT

---

17. Was/is notice provided to the individual prior to collection of information? No

17b. If **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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? ITOR receives its information directly from other ACA 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

19. 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.

---

## **I. INFORMATION PROTECTION**

---

20. 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

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

IRS Employees? Yes

| <u>IRS Employees?</u> | Yes/No | Access Level (Read Only/Read Write/<br>Administrator) |
|-----------------------|--------|---|
| Users                 | Yes    | Read-Only   |
| Managers              | Yes    | Read-Only   |
| Sys. Administrators   | Yes    | Administrator   |
| Developers            | Yes    | Read-Only   |

Contractor Employees? Yes

| <u>Contractor Employees?</u> | Yes/No | Access Level  | Background Invest.<br>Level |
|------------------------------|--------|---------------|-----------------------------|
| Contractor Users             | Yes    | Read-Only     | Moderate                    |
| Contractor Managers          | No     |               |                             |
| Contractor Sys. Admin.       | Yes    | Administrator | Moderate                    |
| Contractor Developers        | Yes    | Read-Only     | Moderate                    |

21a. 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

---

## **I.1 RECORDS RETENTION SCHEDULE**

---

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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.

---

## **I.2 SA&A OR ECM-R**

---

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail 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.

---

## **J. PRIVACY TESTING**

---

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, 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? ISR-A&R, like other IRS systems, has to conduct a series of tests 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.

24b.1. If **completed**, 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.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

---

#### **K. SBU Data Use**

---

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

25a. If **yes**, was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? No

If **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 a SBU Data Use Request is not required. Formal acceptance of the questionnaire is pending approval.

---

#### **L. NUMBER AND CATEGORY OF PII RECORDS**

---

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

26a. IRS Employees: Not Applicable  
26b. Contractors: Not Applicable  
26c. Members of the Public: Not Applicable  
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000). More than 100 million records containing TCC.

---

**M. CIVIL LIBERTIES**

---

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

---

**N. ACCOUNTING OF DISCLOSURES**

---

30. 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

---

**End of Report**

---