
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. PGLD:PPC:IM Incident Data Storage, IM ITIM

2. Is this a new system? No

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

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

- No 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? _

If yes, explain what changes were made.

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? Yes

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.

Electronic recordation of reported incidents addressed by the Incident Management (IM) Team. Access is managed by an IM Team designee via the IT Help Desk.

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.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

<u>Yes</u>	Social Security Number (SSN)
<u>Yes</u>	Employer Identification Number (EIN)
<u>Yes</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>No</u>	Practitioner Tax Identification Number (PTIN)

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

The system requires the use the full SSN and a mitigation strategy is currently not required. No alternative exists currently for the application. as the SSN is the key data element for the legal response required by Office of Management and Budget (OMB). This program is aware of and part of the IRS-wide SSN elimination and reduction program.

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? No

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

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>No</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>Yes</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>Yes</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	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 this criteria. Be specific.

The IRS is required by OMB guidance to have an Incident Response Plan that includes assessing the risk of ID theft or other harm relative to losses, thefts or disclosures of personally identifiable information (PII) from IRS sources (employees, systems, etc.) and notifying those individuals deemed "likely" to be potential victims. The key data elements are name, address, SSN. The IMT retains the notification material to address undelivered or letter re-issuance, and document event activity. There is an established access process AND records disposition schedule.

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 Sensitive but unclassified (SBU)/PII data is reported to the IMT as the information leaving IRS control. Consequently, the entity information is gathered and validated as the latest name/address via IRS Masterfiler, the requisite location for this. The nature of this program must rely on the tax account entity information as the sole source. There are no systemic interactions.

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? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number

SORNS Name

Treas/IRS 34.037 Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. *Redacted Information For Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? 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, cloud, 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.
Information is received from IRS staff directly related to the incident but not the impacted individuals.
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? This data is collected and stored in relation to the IRS response to loss, theft or disclosure and retention is necessary to support organizational activity.
19. How does the system or business process ensure due process regarding information access, correction and redress?
This data is in direct response to potential affect for individuals. Data is either employee or taxpayer owned and comes as a result of employment or tax return submission.

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/Administrator)
Users	Yes	Read and Write
Managers	No	
Sys. Administrators	No	
Developers	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? An IM Team member is designated as the responsible party. Requests are made and analyzed based on need and use. User access to data is determined by need-to-know requirements managed by an IMT staff member. The criteria, procedures, controls and responsibilities regarding access comply with the Computer Security Act of 1987's standards and guidelines on security and privacy. Approved access is ONLY for IMT members processing reported incidents. The IMT responsible party must approve requests for access based on a need-to-know and the list of those approved is reviewed semi-annually and stale users are deleted. IMT approved users have access to view historical data and add case information. User access is given through the Online 5081 (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 records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. For different data types, there are different retention periods. Retention schedules are documented in the Functional specific schedules, and are scheduled separately. ITAMS records are scheduled in RCS 17, Item 23 and e-Trak is scheduled in RCS 33, Items 10-12. IDRS letters and records are scheduled in RCS 29, Items 236-283. Any records stored in the IM ITIM files will be managed according to requirements under IRM 1.15.1, GRS 4.3 item 010 for input and source records, and will be scheduled using IRS Records Control Schedules (RCS) 8, 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. Existing Audit Trails for IRS networks and common drives. Access is monitored by an IM Analyst and the process is handled by the IRS Help Desk. Encryption is employed when/where possible and applicable.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. This is a shared/common drive established throughout the IRS. IMT staff use this drive to house supporting material. There is no software nor added hardware.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees:	<u>Under 50,000</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>100,000 to 1,000,000</u>
26d. Other:	<u>No</u>

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
