
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Integrated Collection System, ICS

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.

Integrated Collection System (ICS), O&M

Next, enter the **date** of the most recent PIA. 9/19/2013

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
- Yes 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? 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.

The ICS application is a case management system that supports the IRS SB/SE Revenue Officers (RO) in working delinquent tax cases. An ICS RO works directly with the delinquent taxpayer by mail, phone, and face-to-face meetings to resolve the delinquent tax case.

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 No On Dependent

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

- Yes Social Security Number (SSN)
- Yes Employer Identification Number (EIN)
- Yes Individual Taxpayer Identification Number (ITIN)
- No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
- Yes 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).

ICS has already redacted TINs wherever it is practical to do so.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No

Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
No	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

If **yes**, describe the other types of SBU/PII that are applicable to this system.

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>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	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 this criteria. Be specific.

The ICS application provides an automated system for Revenue Officers (ROs), Group Managers (GM), and support staff to process and store delinquent taxpayer case data in the resolution of delinquent tax cases assigned to the SB/SE Collection Division. The ICS application supports approximately 7,500 Small Business/Self-Employed (SB/SE) users including Collection Field, Campus, Insolvency, Appeals, and Taxpayer Advocate Service end users.

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

Data is visually inspected and corrected manually when errors are encountered. Validity checks for timeliness and completeness are completed on the data prior to and while it is loaded in the ICS. Information that has significance to a determination of a tax liability or a penalty is verified by looking at bank records, corporate files, and other official sources. Information pertaining to the taxpayer's financial situation is verified by reviewing courthouse records and by contacting creditors to verify balances due. The investigator then keys the information into the ICS. Appropriate validity and consistency checks are built into the automated system.

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 IRS Audit Trail and Security Records Systems

Treas/IRS 24.030 CADE Individual Master File (IMF)

Treas/IRS 24.046 CADE Business Master File (BMF)
 Treas/IRS 26.009 Lien Files, (open and closed)
 Treas/IRS 26.013 Trust Fund Recovery Case/One Hundred Percent Penel
 Treas/IRS 26.019 Taxpayer Delinquent Account (TDA) Files
 Treas/IRS 26.020 Taxpayer Delinquency Investigation Files
 Treas/IRS 36.003 General Personnel and Payroll Records
 Treas/IRS 44.003 Appeals Centralized Data System (ACD)

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? 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 & A?</u>	<u>Authorization Date</u>
Business Master File (BMF) Outputs	Yes	02/24/2015	Yes	05/04/2015
IDRS	Yes	08/03/2014	Yes	12/05/2014
ACDS	Yes	02/02/2015	Yes	03/24/2014
Compliance Data Warehouse (CDW)	Yes	12/13/2012	No	03/24/2014
Centralized Authorization File (CAF)	Yes	08/03/2014	No	03/24/2014
Daily TIF Update (DLY)	Yes	08/03/2014	No	03/24/2014
Embedded Quality Review System-Field (EQRS-NQRS-FIELD)	Yes	03/16/2016	Yes	03/09/2015
Penalty and Interest Explanation (PINEX)	Yes	08/03/2014	No	03/09/2015
Reporting Agents File (RAF)	Yes	08/03/2014	No	03/09/2015
Taxpayer Delinquency Investigation (TDI)	Yes	08/03/2014	No	03/09/2015
Third Party Contact (TPC)	Yes	08/22/2014	Yes	11/04/2014
Weekly TIF Update (WTU)	Yes	08/03/2014	No	11/04/2014
Automated Trust Fund Recovery System (ATFR)	Yes	02/10/1914	Yes	05/29/2015

ALS ENTITY

Yes

11/12/2013

Yes

10/20/2015

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 (-ies)? 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 & A?</u>	<u>Authorization Date</u>
Customer Satisfaction Survey (CSTS)	Yes	10/03/2012	No	
Integrated Data Retrieval System (IDRS)	Yes	08/03/2014	Yes	12/05/2015
Automated Trust Fund Recovery System (ATFR)	Yes	02/10/2014	Yes	05/29/2015
Enforcement Revenue Information System (ERIS)	Yes	03/31/2015	Yes	05/23/2012
Embedded Quality Review System(EQRS)	Yes	03/16/2016	Yes	03/09/2015
Inventory Delivery System (IDS)	Yes	01/15/2014	Yes	09/24/2015
Service-wide Electronic Research Project (SERP)	No	01/15/2014	No	09/24/2015
Standard IDRS Access (SIA) Tier II	Yes	12/17/2014	Yes	09/27/2012
ALS ENTITY	Yes	11/12/2013	Yes	10/20/2015
Integrated Collection System Data Store (ICSIDS)	Yes	09/19/2013	No	10/20/2015
Third Party Contact Database (TPC)	Yes	08/22/2014	Yes	11/04/2014
Centralized Authorization File (CAF)	Yes	08/03/2014	No	11/04/2014
Reporting Agents File (RAF)	Yes	08/03/2014	No	11/04/2014

Identify the authority and for what purpose? CSTS – To provide information to conduct customer satisfaction surveys IDRS (via SIA) – To upload transactions ATFR – To provide data in generating Trust Fund Recovery Assessments ERIS – To provide information which allows the IRS to report revenue and direct time information to its overseers, the Treasury Department, the

Office of Management and Budget, the Government Accountability Office, and U.S. Congress ICSDS – Storage of Archival ICS data EQRS – For quality review purposes IDS – Allows flow of ICS cases for management purposes SERP – POD and assignment information provided customer service (toll free) operation SIA Tier II - It uses data from the Taxpayer Information File Data Store (TIF DS) and from various Corporate Files On Line (CFOL) files to validate data provided by various other application systems. ALS – To generate Notice of Federal Tax Liens ENTITY – For purpose of generating reports and data query capabilities TPC - 3rd Party Contact Database – To record collection contacts with third parties CAF - Centralized Authorization File (CAF) (weekly refresh requests) RAF - Reporting Agents File (RAF) (weekly refresh requests)

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, 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.

The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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? The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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

The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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	Yes	Read and Write
Sys. Administrators	Yes	Read-Only
Developers	Yes	Read-Only

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? A potential user will request access via the OL5081 system. This request has to be approved by the potential user's manager based on a user's position and need-to-know.

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.

ICS data is currently approved for destruction three years after processing or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner (Job No. N1-58-97-13). Disposition instructions are published in IRM 1.15.35, item 29 (pending publication in new IRS Document 12990 under RCS 35, item 29). Current business unit practice dictates that when a taxpayer case is closed, the closing information is made part of the taxpayer records on the IDRS and Master

File. The case is maintained on the ICS mainframe as a closed case for six months, after which portions of the closed case are archived. The archived files are available for three years and then destroyed. Any backup files maintained by the system are destroyed at the end of their retention period, which is documented in the Computer Programmer Books (CPBs) used at the Computing Centers. The procedures for disposing of closed cases are contained in IRS Document 12990, RCS 28.

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)? Yes

23a. If **yes**, what date was it completed? 3/23/2016

23.1 Describe in detail the system's audit trail. ICS has an approved Audit Plan but it is not complete until it has been implemented. This would include having an approved Interface Control Document (ICD) to send our audit information to ESAT/SAAS. The audit trail contains the audit trail elements as required in current IRM 10.8.3, Audit Logging Security Standards.

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?

A review of the Privacy Requirements against the Integrated Collection System (ICS) produced the following results: 1. Accountability Confirmed: All ICS user actions and program messages are captured and stored in ICS log files. 2. Purpose Limitation Confirmed: All PII information collected and stored for ICS are necessary to support the ICS business purposes of tax collection. 3. Minimizing Collection, Use, Retention and Disclosure Confirmed: ICS PII data is restricted to the Production and Development systems. Only sanitized production data is used on the Training system. ICS data is currently approved for destruction 3 years the case is 'confirmed closed': after attaining that status, a case remains on the 'active' ICS database for six months, and if it is not reopened during that timespan, it is archived (put in 'archive' status). It is then deleted from the archive after two-and-a-half years if there is no related case on the 'active' ICS database during that timespan (note that a case may be accessed while in archive status but that does not change the two-and-a-half year limit). If, however, a case related to an archived case appears on the 'active' ICS database (such a case can be open or closed), the related archived case is not deleted until the related 'active' case reaches archive status, upon which data from the two cases is combined and the two-and-a-half year archive clock begins anew. Retention instructions specific to ICS are contained in IRM 1.15.35. 4. Openness and Consent Confirmed: The Privacy Act Notice 609 is presented during the initial interview with a taxpayer and/or with the initial distribution of various Collection forms and letters sent to the Taxpayer. 5. Strict Confidentiality Confirmed: Access to ICS data is limited to authorized ICS users and is made available on a need to know basis. The employee must fill out an Online Form 5081 (OL5081) to request access to ICS and based on the employee's position and access level will be approved by the appropriate manager. Employee access to ICS data is terminated once their duties no longer require access to the ICS system. 6. Security Confirmed: The PII data collected and input

into ICS includes taxpayer information related to TDAs and TDIs, employee information for assigning cases, generating documents and correspondence and Audit trail information about each action taken. 7. Data Quality Confirmed: Prior to the release of application software into the production environment, extensive testing is performed by the Development staff and Systems Acceptability Testing (SAT) is performed by the Enterprise System Testing staff (EST). ICS uses data validation and business rules to ensure valid data is entered into a field. The application will generate an error message if required fields are left blank or are missing information. Information that has significance to a determination of a tax liability or a penalty is verified by looking at bank records, corporate files and other official sources. 8. Verification and Notification Confirmed: The PII data collected for tax administration is received from IDRS, BMF, CADS, EQRS, ALS and ACDS. In addition, information may be gathered from public records and from the taxpayer during personal interviews. The Internal Revenue Code (IRC) 6331 authorizes levies to collect delinquent tax. Before property can be levied, the taxpayer must be given a 1) Notice and demand - IRC 6303(a); 2) Notice of intent to levy, and - IRC 6331(d) and 3) Notice of a right to a Collection Due Process (CDP) hearing – IRC 6330. The Letter 1058 contains the information required by Treasury Regulations and the Internal Revenue Code. 9. Access, Correction and Redress Confirmed: The PII data collected in ICS can be modified with updates and corrections as necessary until the Case is Closed. 10: Privacy Awareness and Training Confirmed: All IRS employees undertake annual Privacy Awareness and Unauthorized Disclosure (UNAX) training.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Results are stored in DocIT.
<http://nct0010cp642188/docit/component/main?dmfClientId=1460492275242&dmfRequestId=client1~~2&dmfJumpType=jump>

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? Yes

If **yes**, provide the date the permission was granted. 3/23/2016

25b. If **yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: Not Applicable
26d. Other: No

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
