Integrated Collection System (ICS) – Privacy Impact Assessment

PIA Approval Date – December 15, 2010

System Overview:
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. The ICS contains privacy information related to a taxpayer delinquent account (TDA) or taxpayer delinquent investigation (TDI). TDA and TDI information is extracted from the Integrated Data Retrieval System (IDRS) or may be input into the system by users of ICS. Information such as liens, levies, levy sources, assets, seizure activity, address, Power Of Attorney (POA), payments, as well as closing information and history may be added to the case file by users of ICS and then uploaded to IDRS. Information such as name and taxpayer identification number (TIN) is not uploaded, since such information is already contained within IDRS.

Systems of Records Notice (SORN):

- Treasury/IRS 24.030, CADE Individual Master File (IMF)
- Treasury/IRS 24.046, CADE Business Master File (BMF)
- Treasury/IRS 26.009, Lien Files, (open and closed)
- Treasury/IRS 26.013, Trust Fund Recovery Case/One Hundred Percent Penalty Cases
- Treasury/IRS 26.019, Taxpayer Delinquent Account (TDA) Files
- Treasury/IRS 26.020, Taxpayer Delinquency Investigation Files
- Treasury/IRS 34.037, IRS Audit Trail and Security System
- Treasury/IRS 36.003, General Personnel and Payroll Records
- Treasury/IRS 44.003, Appeals Centralized Data System (ACD)

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – The ICS contains information related to a TDA or TDI. TDA and TDI information is extracted from the IDRS or may be input into the system by users of ICS. Information such as liens, levies, levy sources, assets, seizure activity, address, POA, payments, as well as closing information and history may be added to the case file by users of ICS and then uploaded to IDRS. Information such as name and TIN are not uploaded, since such information is already contained within IDRS.

B. Employee – Minimal employee information is stored on the system for the purpose of assigning the taxpayer cases to them and generating documents and correspondence. Employee information includes the following:

- Employee's name
- Work address
- Work telephone number
- E-mail address
- Title
- Grade
- Identification number

C. Audit Trail Information – Audit trail information about each action taken on a case is captured and stored. The ICS application has a Windows XP workstation component and an IBMIAP mainframe component. The ICS end user does not 'login' to the IBMIAP mainframe component. Identification and authentication are done at the local area network (LAN) level using the Active Directory. The end user's LAN account (Standard Employee Identifier-SEID) must be in the ICS_USERS Active Directory group. The audit logs for ICS access are performed by the Active Directory Domain Controller.

D. Other – ICS does not contain any other data.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – IDRS, Business Master File (BMF) and the Automated Lien System (ALS) are the sources of data relating to a taxpayer on the system. Corporate Authority Directory Service (CADS) is the source of the employee's email address.

B. Taxpayer – Case information may be gathered from the taxpayer during an investigation. This information may contain taxpayer's income, expenses, assets and liabilities. Once gathered, it is keyed into the system by ICS users.

C. Employee – Case information is gathered by IRS employees during field investigations. This information is based on a review of public records or obtained from the taxpayer during personal interviews.

D. Other Federal Agencies – The ICS application does not obtain data elements from other Federal agencies.

E. State and Local Agencies – The ICS application does not obtain data elements from State and Local agencies.

F. Other Third Party Sources – Revenue Officers will contact other third party sources (creditors, neighbors, employers, former employers, etc.) to secure information.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items are necessary to support the ICS's business purposes. Each user receives their case inventory electronically and then is able to work the case electronically (i.e., contacting the taxpayer, generating correspondence, issuing liens and levies, closing cases and posting payments). Reports are produced using the information in the system.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Data will be 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.

5. Is there another source for the data? Explain how that source is or is not used.
No. There are no other sources of data.

6. Generally, how will data be retrieved by the user?
The ICS system makes the data available to users on a need-to-know basis. All SB/SE Collection Field function, Centralized Case Processing, and Advisory, Insolvency, & Quality employees and their managers who work or manage an inventory of cases are allowed access to their inventory. Users have access to taxpayer case details and case history information by accessing the ICS application on their laptops and workstations. The information is displayed by using the application hierarchal set of menus.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. A user's inventory of data is displayed/ presented to them via a unique assignment number that is tied to their unique identifier. A given case in their inventory may then be selected. Also, a specific case not part of an employee's assigned inventory may be requested by Employer Identification Number (EIN) or Social Security number (SSN). An employee's SEID is used to retrieve his/her e-mail address.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

- **Roles:** SB/SE Collection Field function, Centralized Case Processing, and Advisory, Insolvency, & Quality employees and their managers.
- **Permissions:** Users are allowed access to their inventory by name and can access data on another account by EIN and SSN.

- **Roles:** Users in other functions.
- **Permissions:** Users may access data on a specific taxpayer's account by EIN or SSN.

- **Roles:** Developers
- **Permissions:** Users may access data on a specific taxpayer's account by EIN or SSN.

9. How is access to the data by a user determined and by whom?
The employee must fill out Online Form 5081 (OL5081), Information System User Registration/Change Request, to request access to the application. Based on the user's position and their access level, the manager will approve the request and the user will be added. A user's access to the data terminates when the user no longer requires access to the system to perform their duties. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on OL5081.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. The ICS receives information from IDRS, Business Master File (BMF), Taxpayer Delinquent Investigation (TDI) (part of IDRS), CADS, Embedded Quality Review System (EQRS), Entity, Automated Lien System (ALS),and Appeals Centralized Database Systems (ACDS). The ICS provides information to Entity, Servicewide Electronic Research Program (SERP), Standardized IDRS Access (SIA), Enforcement Revenue Information System (ERIS), ALS, IDRS, Automated Trust Fund Recovery (ATFR), Inventory Delivery System (IDS), Pacific Consulting Group – survey data, and the Third Party Contact (TPC) database. The ICS does not share information with another system.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.

Appeals Centralized Database Systems (ACDS)
- Certification and Accreditation (SA&A) – 4/18/2008
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 1/10/2008

Automated Lien System (ALS)
- Certification and Accreditation (SA&A) – 3/24/2008
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 11/17/2010

Automated Trust Fund Recovery (ATFR)
- Certification and Accreditation (SA&A) – 12/22/2008
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 5/27/2008

Business Master File (BMF)
- Certification and Accreditation (SA&A) – 6/14/2010
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 3/16/2010

CADS (Part of the MITS-17 Accreditation Boundary)
- Certification and Accreditation (SA&A) – 9/24/2010
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 2/19/2010

Embedded Quality Review System (EQRS)
- Certification and Accreditation (SA&A) – 6/7/2010
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 3/16/2010

Enforcement Revenue Information System (ERIS)
- Certification and Accreditation (SA&A) – 5/7/2009
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 3/5/2009

Integrated Data Retrieval System (IDRS)
- Certification and Accreditation (SA&A) – 3/10/2009
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 10/31/2008

Inventory Delivery System (IDS)
- Certification and Accreditation (SA&A) – 5/1/2009
  Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 9/10/2008

Pacific Consulting Group (PCG)

- Certification and Accreditation (SA&A) – N/A per Cybersecurity Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – N/A per Cybersecurity

Servicewide Electronic Research Program (SERP)

- Certification and Accreditation (SA&A) – 5/5/2008 Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 3/6/2008

Standardized IDRS Access (SIA)

- Certification and Accreditation (SA&A) – 10/5/2009 Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 5/20/2009

Taxpayer Delinquent Investigation (TDI) Odyssey (part of IRDS)

- Certification and Accreditation (SA&A) – 3/10/2009 Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 10/31/2008

Third Party Contact (TPC)

- Certification and Accreditation (SA&A) – 4/21/2009 Authority to Operate (ATO)
- Privacy Impact Assessment (PIA) – 1/30/2009

12. Will other agencies provide, receive, or share data in any form with this system?
No. Other agencies will not provide, receive, or share data in any form with the ICS.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
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, item 39, and published under IRM 1.15.35, 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 the Internal Revenue Manual 1.15.28. Retention instructions specific to ICS are contained in IRM 1.15.35, as noted above.

14. Will this system use technology in a new way?
No. The ICS does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. The ICS is a case management system that supports the IRS SB/SE Revenue Officers (RO) in working delinquent tax cases. Users may obtain taxpayers' addresses of record for cases on the ICS and may use the system to generate correspondence for the purpose of locating taxpayers.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
Yes. The ICS is used to monitor the compliance of taxpayers with accounts on the ICS, including Federal Tax Deposit (FTD) compliance, compliance with established deadlines, and to maintain a history of actions taken on an account. Access to the ICS is limited to authorized users approved via OL5081, Information System User Registration/Change Request. Access to the data within the system is determined by a user's assigned role and audit logs capture user transactions.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. All IRS policy and guidelines related to taxpayers are applicable to all taxpayers.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. For example, a taxpayer may claim a payment has been made and that is not reflected on the account. Research would be conducted and corrections requested as appropriate.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
ICS is not a web-based system. Therefore, it does not use persistent cookies or other tracking devices to identify Web visitors.

View other PIAs on IRS.gov