

# Automated Collection System (ACS) – Privacy Impact Assessment

PIA Approval Date – Feb. 5, 2007

Requested Operational Date – ACS is currently in production

## System Overview

Automated Collection System (ACS) accepts Integrated Data Retrieval System (IDRS) balance due and nonfiler cases requiring telephone contact for resolution, and generates levies and correspondence. Tax Examiners use ACS' case management abilities to contact taxpayers, review their case histories, and issue notices, liens, or levies to resolve the cases. Taxpayer contact is accomplished through incoming and outgoing telephone calls via Automated Call Distributor (ACD) and through correspondence to taxpayers and third parties.

## Systems of Records Notice

- IRS 26.019 Taxpayer Delinquent Accounts (TDA) Files including subsystems as the System of Records for ACS.
- Treasury/IRS 34-137 IRS Audit Trail and Security Records System

## Data in the System

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

- A. Taxpayer:** Taxpayer Information available in ACS pertains to Taxpayer Delinquency Account (TDA) and Taxpayer Delinquency Investigation (TDI) data and provides: name of taxpayer (if married, spouse personal information), home address, DOB, home telephone number, personal cell number, work telephone number, Tax Identification Number (TIN), account information relating to tax liabilities, information regarding liens, levies, levy sources, assets, partnership and/or corporation name, and Power of Attorney (POA) telephone number.
- B. Employee:** Employee information is stored on the system for the purpose of assigning taxpayer cases, controlling workload, and generating documents and correspondence. Files include employees name, office location, ACS employee number, Resource Access Control Facility (RACF) ID and type of access permission allowed.
- C. Audit Trail Information:** For each auditable event the audit trails captures the date and time that a particular event occurred; the users unique identifier (e.g., employee number and RACF ID) or the application initiating the event; type of event; subject of the event (e.g., the user, file, or other resource affected) and the action taken on that subject; the outcome status (success or failure) of the event, date and time of input, TIN, Master File Tax (MFT), and tax period.

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

- A. IRS:** ACS obtains data from Corporate Files Online (CFOL) system, Integrated Data Retrieval System (IDRS), Inventory Delivery System (IDS) and Electronic Levy System.
- CFOL provides: DOB and adjusted gross income
  - IDRS provides: Taxpayer name, address, TIN
  - IDS: home address, telephone number, TIN
  - ELS: Levy source information (third party information); levy source name, address, TIN, and the phone number of the actual levy source.
- B. Taxpayer:** Customer Service Representatives (CSRs) contact taxpayers by telephone to update and receive additional taxpayer information such as: name of taxpayer (if married, spouse personal information), home address, DOB, home telephone number, personal cell

number, work telephone number, Tax Identification Number (TIN), account information relating to tax liabilities, information regarding liens, levies, levy sources, assets, partnership and/or corporation name and POA telephone number

**C. Other third party sources:** In the CSR's attempt to locate taxpayers that may have moved, a letter is sent to the prior taxpayer's neighbors requesting them to provide knowledge (if known) of the taxpayer's new address and telephone number and supply this information by mail or call the number provided in the letter.

**3. Is each data item required for the business purpose of the system? Explain.**

Yes. The business purpose for each data item is required to assist with the collection of delinquent accounts through automated contact with delinquent taxpayers.

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

ACS applies various methods to check for information accuracy, completeness, and validity. ACS application performs extensive field checking on the data manually entered by the end user. This includes checking for content and syntax. The ACS Real Time screens have built in procedural checks and error messages are displayed for the end users. Application error messages are documented in ACS Hummingbird folders; a records management tool that provides a secure environment to manage and protect the complete lifecycle of enterprise information.

Users normally report errors to the Help Desk by means of the Inventory Technology Asset Management System (ITAMS) process. This process then notifies the ACS application programmers that diagnose and correct the discovered errors. On occasion, when circumstances warrant, users report errors directly to the ACS application programmers, who log, diagnose and correct the problem.

In addition, DI catches and displays error conditions in a real-time manner whenever possible. All calls are synchronous and return a success or failure message before more actions are taken on DI. There are several different screens that display different types of error conditions (Information, Warning or Critical Failures). Since ACSWeb utilizes DI, these errors also apply to errors related to ACS.

**5. Is there another source for the data? Explain how that source is or is not used.**

No. There is no other source for the data

**6. Generally, how will data be retrieved by the user?**

Only authorized users can access the ACS test or production environments. Employee ID and password are authenticated prior to accessing the system.

Users have access to specific inventory of taxpayer accounts which are determined when the user logs onto the system. The employee number, team, function, and unit assigned determine the access to the inventory. This information is stored in the Security database.

Once added to the ACS database by a site Systems Administrator (at least 1 SA per site), the representative may access accounts in several manners. They may access via the "Next Case" option built into the ACS system. They are able to hit the next case key (F2) and will be given the next available account depending on the Team/Function/Unit that they are signed on to. They may also access accounts based on a Taxpayer Identifying Number or an Employer Identifying Number (TIN/EIN) depending on whether the account is an IMF or BMF account. They are also able to access when taking incoming calls and are given the TIN/EIN by the taxpayer. Correspondence may also give them a TIN/EIN or case reference number to access the account.

## **7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?**

Yes. The user first logs into the system by entering his/her RACF User ID, password, or ACS employee number. Authorized users then enter TIN and case reference number to retrieve taxpayer data.

### **Access to the Data**

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

The following users have access to the data in the system:

- **Computer Systems Analyst (CSA)/System Administrator:** Level II/Tier II support for problem resolution. CSA's have Read/Write access to operating system.
- **Operator/Database Analyst (DBA) User:** When a job is released, Operators mount tapes and monitor the jobs being run. They handle print operations and respond to console messages. They have Read/Write access to all application data.
- **Application Developers:** Application Developers are authorized to use ACS with limited Read/Write access to data.
  - ACS contractors only hold the role as Developer.
- **ACS End Users:** National (N) Office-
  - Super users have full access and can modify application parameters.
  - Master (M) – Can add users and review parameter tables. Can review audit logs (in Control-D Web).
  - Supervisor (S) – Manage functionality but can not add users to ACS.
  - Can review audit logs (Control-D Web).
  - Operator (O) – Access taxpayer accounts, issue correspondence, issue levies, issue liens, etc. Input comments. Add financial information.

## **9. How is access to the data by a user determined and by whom?**

Unique mainframe usernames and passwords are required for system authentication. An OL5081 is required of IRS users requesting access to ACS, via the IBM mainframe, and must be signed by an immediate manager. Once forms are approved they are submitted to the system administrator, who adds the new user's account into the system. The OL5081 process ensures that the user identifier is issued to the intended party and that user identifiers are archived. These archives are stored in the OL5081.

Once credentials are received by the user, they sign into the OL5081 with unique username and password, then a Manager approves it before they have access to ACS. Along with OL5081, RACF and IDRS also verify the identity of the user.

User accounts are disabled after 45 days of inactivity, and removed after 90 days.

Contractors that have access to ACS as Developers, have a minimum background investigation level.

## **10. Do other IRS systems provide, receive, or share data in the system?**

Yes. ACS interfaces with numerous applications that send data to ACS and receive data from ACS.

### **The following applications send data to ACS.**

- **Electronic Levy System (ELS)-** is an online levy notice review which screens, updates outgoing mailing addresses and flag notices. Data is sent weekly and automatic.

Input: ACS receives the National Unload Levy Files (3 in all) onto ACS. The data includes third party levy source information.

Output: ACS File Transfer Protocol (FTP) files to the ELS system on the Sun Machine and the file contains levy records with name, address and levy source information.

- Standard IDRS Access (SIA Tier II)- An error file is sent containing TIN, name control (first 4 letters of last name) and tax period. Data is sent daily and automatic.
- DI- TIN, Data is sent daily and automatic.
- IDRS/Taxpayer Information File (TIF)-
- TDA and TDI data, name of taxpayer (if married, spouse personal information), home address, DOB, home telephone number, personal cell number, work telephone number, TIN, account information relating to tax liabilities, information regarding liens, levies, levy sources, assets, partnership and/or corporation. Data is sent weekly and automatic. The below data files contains information extracted from IDRS database.
- Daily Transaction Register (DTR)-  
Obtains information from IDRS. The DTR tape contains, Taxpayer TIN, File Source and TIN Type, along with Module Balance. The Taxpayer data is written to ACS Call Site based on the Area Office Territory Office (AOTO) field which specifies which call site the data belongs.
- Taxpayer Delinquent Account (TDA)- The TDA tape contains TIN numbers, TIN module status, module balance, taxpayer name, address, phone numbers, spouse name, address, penalty amount, interest accrual amount, and various indicators.
- Taxpayer Delinquency Investigation (TDI)- The TDI tape contains TIN numbers, TIN module status, module balance, taxpayer name, address, phone numbers and last amount filed.
- ACS Web-TIN, and pushes transactions to ACS daily and automatic.
- CFOL- DOB, balance due, adjusted gross income amount, SSN and address. Data is sent weekly and automatic.
- Centralized Authorization File (CAF)- Telephone numbers for taxpayers are retrieved from the CAF database and for TIN that have CAF indicator alert set on his/her account. ACS will update phone numbers on the database where taxpayer data is stored. POA, name, and address are retrieved and used to produce correspondence, but not permanently stored on ACS. Data is sent daily and automatic.

POA is retrieved from CAF and used to produce correspondence, but not permanently stored on ACS. Data is sent daily and automatic.

- Inventory Delivery System (IDS)/Telephone Number Research (TNR) telephone- TIN, telephone numbers. Data is sent weekly and automatic.
- Predictive Dialer-TIN. Data is sent daily and automatic.
- Global Information Infrastructure (GII)-TIN.
- Office of Information Technology at Treasury (OIT)- name of taxpayer (if married, spouse personal information), home address, DOB, home telephone number, personal cell number,

work telephone number, TIN, account information relating to tax liabilities, information regarding liens, levies, levy sources, assets, partnership and/or corporation name, and POA telephone number. Data is sent monthly and automatic.

- Integrated Customer Communications Environment (ICCE)-zip code information for a disaster event (does not relate to taxpayers). Data is sent weekly. Data may be sent only once or twice a year. The automated process retrieves data from ICCE on a weekly basis (if data exist).

**The following applications receive data from ACS.**

- IDS-TIN. Data is received weekly and automatic.
- Third Party Contact (TPC)- TIN, name of taxpayer and address. Data is received daily and automatic.
- ACSWeb- Telephone number and TIN. Data is received daily and automatic.
- SIA- TIN, tax account information such as MFT and tax period. Data is received daily and automatic.
- IAP (ICS/ACS/PRINT)-TIN, name and address. Sends information to the print system. Data is received daily and automatic.
- Appeals Centralized Database System (ACDS- All taxpayer data elements within ACS. Data is received daily and automatic.
- Dell NT Sever Austin Service Center(AUSC)-TIN, name, address, MFT and tax period. Data is received daily and automatic.

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

Yes.

ELS:

- Certification & Accreditation (C&A) approved on January 12, 2006, expiring January 12, 2009.
- Privacy Impact Assessment (PIA) approved on April 8, 2005, expiring April 8, 2008.

Standard IDRS Access (SIA Tier II):

- C&A approved on February 10, 2006, expiring February 10, 2009.
- No PIA.

DI:

- C&A approved on May 30, 2006, expiring May 30, 2009.
- PIA approved on December 17, 2003, expiring December 17, 2006.

IDRS/TIF:

- C&A approved on May 18, 2006, expiring May18, 2006.
- PIA approved on April 27, 2005.

DTR:

- C&A approved on May 18, 2006, expiring May 18, 2009.
- PIA approved on April 27, 2005, expiring April 27, 2008.

TDA:

- C&A approved on May, 18, 2006, expiring May 18, 2009.
- PIA approved April 27, 2005, expiring on April 27, 2008.

TDI:

- C&A approved on May 18, 2006, expiring May 18, 2009.
- PIA approved on April 27, 2005, expiring April 27, 2008.

ACS Web:

- C&A approved on August 20, 2004, expiring on August 20, 2007.
- PIA approved on July 17, 2003, expired July 17, 2006.

CFOL:

- No C&A or PIA.

CAF:

- C&A approved on May 18, 2006, expiring May 18, 2009.
- PIA approved on September 24, 2004, expiring September 24, 2007.

IDS:

- C&A approved on June 2, 2006, expiring on June 2, 2009.
- PIA approved on June 2, 2003, expired June 2, 2006.

Predictive Dialer:

- C&A approved on August 31, 2006, expiring August 31, 2009.
- PIA approved on December 10, 2003, expiring December 10, 2006.

GII:

- No C&A or PIA.

OIT:

- No C&A or PIA.

ICCE:

- No C&A.
- PIA approved on October 1, 2003, expired on October 1, 2006.

TPC:

- C&A approved on June 2, 2006, expiring June 2, 2009.
- PIA approved on April 19, 2006, expiring April 19, 2009.

IAP (ICS/ACS/PRINT):

- C&A approved on August 31, 2006, expiring August 31, 2009.
- PIA approved on May 10, 2006, expiring May 10, 2006.

ACDS:

- C&A approved on April 29, 2005, expiring April 29, 2008.
- No PIA.

Dell NT Sever (Austin Service AUSC):

- No C&A or PIA.

**12. Will other agencies provide, receive, or share data in any form with this system?**

Yes. Treasury Inspector General for Tax Administration (TIGTA) annually receives data from ACS.

**Administrative Controls of Data**

**13. What are the procedures for eliminating the data at the end of the retention period?**

When a taxpayer's case is closed, the information is made part of the taxpayer record of IDRS and Master File. The case is maintained on the ACS Mainframe as an archived case for 2 years in accordance with Internal Revenue Manual (IRM) 1.25.28-1, part V.

**14. Will this system use technology in a new way?**

No. ACS 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. Customer Service Representatives use ACS case management functionalities to contact taxpayers, review case histories, and issue notices, liens, or levies in efforts to resolve unsettled cases as part of the business purpose.

**16. Will this system provide the capability to monitor individuals or groups?**

Yes. Customer Service Representatives have the ability to monitor taxpayers cases in order to initiate taxpayer calls, display all relevant information regarding a taxpayer delinquency, issue a variety of letter correspondence to either the taxpayer or third party sources, document conversations with taxpayers, and schedule the account for future follow-up review or other activity as part of the business purpose.

In addition, ACS has the ability to monitor employee workloads and actions taken on cases. The manager has a security profile and can view and monitor individuals or groups of employees.

**17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?**

No. Use of ACS does not allow disparate treatment of taxpayers, employees or others.

**18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?**

Yes. ACS allows the tax examiners to review a taxpayer's history and rectify any issues or inquires by the taxpayer.

Additionally, Customer Service Representatives are available to speak with taxpayers, answer questions, update and correct inaccuracies in an assigned case file.

Customer Service Representatives send letters to taxpayers titled "Notice of Intent to Levy" to warn taxpayer's to respond before enforcement actions are taken.

**19. If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?**

ACS is only accessible by IRS tax examiners. Additionally, there are no persistent cookies or other tracking devices to identify users of the system.

[View other PIAs on IRS.gov](#)