Appeals Customer Service (ACuServ) – Privacy Impact Assessment (PIA)

PIA Approval Date – Dec. 23, 2008

System Overview

The Appeals Customer Service inventory system is called ACuServ – an Intranet web-based system. The purpose of the application is to record all communication with taxpayers or related parties to resolve an account issue. ACuServ enables Appeals Account Resolution Specialists (AARS) to keep inventory control over their Taxpayer Advocate and other closed Appeals cases with account issues. AARS keeps an inventory of cases by Taxpayer Advocates, the Senate Finance Committee, Congress, and other Service Wide Electronic Research Program (SERP) contacts. Additionally, ACuServ is a time accounting system to track various types of general outreach and education activities.

Systems of Records Notice (SORN):

- IRS 44.001--Appeals Case Files
- IRS 44.003--Appeals Centralized Data System (Formerly Unified System for Time and Appeals Records (Unistar)
- IRS 34.037--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 – First Name, Last Name, and Tax Identification Number (TIN) of customers/taxpayers who call the Customer Service Representative or whose representatives call on their behalf.

B. Employee – Employee information is limited to first name, last name, telephone number, and badge number (This number is required to be given to taxpayer and is a disclosable IRS ID number; not the SEID).

C. Audit Trail Information (including employee log-in info) – ACuServ audits the login and logoff of users, change of user password, invalid login attempts, and viewing or modification of any case. For each audit event, the following information is stored:
   - Date
   - Time
   - Username (this is the user's unique logon name.
   - IP address
   - Office code (2-digit Appeals office code)
   - CaseID (the serial number of the case in the case table. Every case has a unique ID.)

   The accessed TIN is not captured in an audit log. In order to determine which user has accessed a particular TIN, a query is run against the database and audit log joining the audit logs with the Case tables/Case ID field. From there, one could tell if a user has accessed a particular TIN. There is only one user per audit log event.

D. Other (Describe) – Information about the calls themselves is also kept. The information stored is: Source Code, Category Code, Satisfaction Code, Closing Code, Customer Contact Dates, and notes from customer contact.

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

A. Taxpayer – Through the CSR or the AARS:
- Taxpayer name
- Tax periods
- Type of tax

B. Employee:
- Name
- Work telephone number
- Badge number

Employee data is stored in a separate table integral to the relational database management system that powers ACuServ.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items are needed for the business purpose of the system. Taxpayer information, including first name, last name, and TIN are used to uniquely identify the account in which the taxpayer has issues. These unique identifiers are used to research the account information in other IRS systems such as ACDS and IDRS in order to resolve account issues. To reiterate, taxpayer information in ACuServ does NOT come from other systems, but rather from the taxpayer or representative or IRS employee. Once that information is received from these sources, the CSR or the AARS can research the other IRS systems to resolve the account issues. Employee information, including name, telephone number, and badge number are needed for locating employees who have dealt with taxpayers on previous calls. Source Code, Category Code, Satisfaction Code, Closing Code, Customer Contact Dates, and notes from customer contact data directly fulfil the business purpose of the ACuServ system. Audit data consisting of the login information is kept for audit trail purposes to identify authorized users accessing ACuServ.

4. How will each data item be verified for accuracy, timeliness, and completeness?
All data in the system is obtained through contact with the taxpayer or his or her representative. The information is validated by the Appeals Customer Service Representatives through the customer.

5. Is there another source for the data? Explain how that source is or is not used.
No. The ACuServ information is attained directly from taxpayers, and is entered into the system by Appeals Customer Service Representatives. ACuServ has no other sources for the data contained in the system.

6. Generally, how will data be retrieved by the user?
The ACuServ application is used by Appeals Customer Service Representatives to document their contacts with customers. ACuServ is accessed over the IRS Intranet by Appeals Customer Service personnel located throughout the IRS. On the ACuServ Home Page, the user will see the ACuServ Top Menu displayed at the top of the screen with these menu options: Add, Update, View, Reports, Administration, Login, and Help. At the bottom of the page is a button labelled Find a Task. If the user clicks this button, they are taken to the Update search screen which has the ACuServ Top Menu still displayed above it. The user can also get to the Update search screen by clicking on Update in the ACuServ Top menu.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier? Yes. Data in the system is retrievable by either taxpayer name or TIN. This is necessary in order to verify identity, and to allow users to retrieve information for repeat callers.

Access to the Data

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

Role: End Users
Permission: Read, Write, Delete

Role: Senior AARS
Permission: Read, Write, Delete

Role: Manager
Permission: Read, Write, Delete

Role: Account Administrator
Permission: Read, Write, Delete

Appeals Customer Service Representatives (users) may add and update tasks and view all tasks in the system, and run reports. There is one permission level among users. An ACuServ Senior Level Customer Service Representative (the Database/System Administrator) is responsible for authorizing, establishing, activating, maintaining, modifying, and removing user accounts. As part of this function, the Account Administrator may add users, assign permissions, update passwords, lock out users, and unlock users who have been locked out, activate accounts, and deactivate accounts. Bug fixes on ACuServ are made by the Developer, after first testing them on a test and development server. If no issues are identified, the developer requests the system administrators move the changed files onto the production server(s). Developers do not have access to the production environment of ACuServ.

No contractors have access to the ACuServ system.

9. How is access to the data by a user determined and by whom?
Users must register for access in OL-5081. The person must first agree to an IRS Registration Agreement that prohibits the person from disclosing information on the website with unauthorized users. Next, the person must fill out a registration form within OL-5081. The OL-5081 system generates a password. OL-5081 e-mails the temp password to the user. Once the user has access to the IRS LAN by following the OL-5081 registration process the user may request an account in ACuServ. An ACuServ Senior Level Customer Service Representative is responsible for authorizing and maintaining the user accounts of ACuServ. The list of Appeals Customer Service Representatives is also published. If an individual requests access and the ACuServ Senior Level Customer Service Representative do not know the individual, a published list of Representatives is referenced to confirm the requestor is an Appeals Customer Service Representative. After an account has been created, the Senior Level Customer Service Representative issues the account information via secure e-mail or in-person. The Senior ACuServ Customer Service Representative (the Database/System Administrator) acts as both end user and administrator.

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. If NO, continue to Question 12.
No. ACuServ has no interconnections with other systems, nor does it share information with other systems.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Not applicable.

12. Will other agencies provide, receive, or share data in any form with this system?
No. No other agencies will provide, receive, or share data in any form with ACuServ.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Four years worth of information is kept in ACuServ. This includes the current fiscal year plus three previous fiscal years. Data for the most distant year is eliminated three years after end of the fiscal year in which a report was prepared as prescribed by IRM Section 1.15.10. Auditing is only performed at the server level and not for the application itself. The server is managed and administered by AP-1. For all AP-1 applications, audit logs are maintained for a minimum period of seven years as prescribed by IRS IRM Section 10.8.3.5.1.9. Electronic marking control data (e.g., signature certificates, private/public keys) are securely maintained. Storage media is sanitized (e.g., overwritten, degaussed, or destroyed) prior to reuse or release. Event logs are archived to CD-ROM on a monthly basis and retained for not less than six years.

14. Will this system use technology in a new way
No. This system 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.
No. This system is not used to identify or locate individuals or groups.

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.
Aside from the audit functionality of the GSS, known as AP-1, as discussed above, the system does not provide the capability to monitor individuals or groups. The only individual with access to the audit records is the Appeals Information Systems Office (AISO) Specialized Programs System Administrators/Database Administrator.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The system is only used for logging contacts with the taxpayer or their representative and does not possess attributes to facilitate the process of making determinations based on information from this system. The Appeals case has already been closed. This system exists solely to service taxpayer complaints.

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

Not applicable. The function of ACuServ is used to keep track of customer complaints. The ACuServ system cannot be used to make decisions that could result in a negative determination. As a result, due process would not be applicable for this system. If the taxpayer is not satisfied with the results of the CSR or AARS action, they can be referred to the Taxpayer Advocates Office, if the case did not originate from there. If the case originated from the Taxpayer Advocates Office, the CSR or the AARS would explain appropriate alternative actions.

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

The system is web based, however the application does not use persistent cookies or other tracking devices. All user activity is either monitored by the application or the underlying operating system.

View other PIAs on IRS.gov