

Date of Approval: September 19, 2016

PIA ID Number: 1751

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Contact Recording, CR

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.

Contact Recording for Taxpayer Assistance Centers (TAC) #576

Next, enter the **date** of the most recent PIA. 7/1/2010

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

<u>No</u>	Addition of PII
<u>Yes</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	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)

<u>No</u>	Vision & Strategy/Milestone 0
<u>Yes</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>Yes</u>	System Deployment/Milestone 5
<u>No</u>	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.

Contact Recording is a premium system responsible for recording 100% of all taxpayer interactions with Internal Revenue Service (IRS) phone agents and a significant sampling of screens as well. These are critical to the business, serving as the basis for employee performance evaluations, performance improvement, and assessments of quality and accuracy. They are also used in National Treasury Employees Union cases, and Treasury Inspector General for Tax Administration and other criminal investigations.

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:

- Yes Social Security Number (SSN)
- Yes Employer Identification Number (EIN)
- Yes Individual Taxpayer Identification Number (ITIN)
- Yes 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).

The CR system only records the audio and screen captures from other IRS systems. The information contained in the recordings is controlled by the contents on the systems used on the representative's workstations. The CR software cannot make any changes to the files once recorded. Any steps to mitigate or eliminate the use of Social Security Numbers (SSN's) would have to come from the other systems that appear on the assistor's computer screen.

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	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
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
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	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	Yes

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
Yes	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
No	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

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

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	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 primary purpose is for quality. The information is collected for Centralized Quality Review System (CQRS). CQRS can evaluate whether the assistor gave the taxpayer a correct answer or not. In order to assist taxpayers, assistors must be able to verify disclosure to access their tax information. This is done by accessing the information and accounts via the taxpayer's SSN.

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 CR system only records the audio and screen captures from other IRS systems. The CR software cannot make any changes to the files once recorded. Any verification would have to come from the other systems that appear on the assistor's computer screen.

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

Treasury/IRS 00.008 Recorded Quality Review Records

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. ##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>
Integrated Automated Technologies (IAT)	Yes	06/18/2013	Yes	06/18/2013
ACSWEB	Yes	12/11/2012	Yes	04/23/2013
Control-D WebAccess (CTDWA)	No	12/11/2012	No	04/23/2013
Integrated Data Retrieval System (IDRS)	Yes	06/07/2012	Yes	12/09/2011
Accounts Management System (AMS)	Yes	03/16/2012	Yes	06/01/2012
Modernized e-file (MeF)	Yes	05/02/2014	Yes	03/01/2013
Field Assistance Queuing Management System (Q-Matic)	No	05/02/2014	No	03/01/2013
Remittance Transaction Research (RTR)	Yes	09/28/2012	Yes	11/28/2012

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? 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? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the

information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
Individuals are provided notification about the collection of the information via a recorded greeting, included here, that says their call may be recorded for quality purposes. Text of recorded message: Your call may be monitored or recorded for quality purposes. Please hold while your call is transferred.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
By asking the assistor to turn off the recording.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Taxpayers can request a copy of a recording by filing a Freedom of Information Act request. Employees will have the opportunity to hear and respond to recordings during feedback sessions, and if appropriate dispute, file a grievance, or pursue litigation as a result of the manager's evaluation.

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-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read-Only
Developers	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Users complete an OL5081 to request access to CR. Part of the job requires accessing Personally Identifiable Information (PII) for IRS systems. Once approved, the user is given a specific profile with controls on what data can be viewed in the CR system. Administrators assign the roles and grant the access level. Administrators cannot modify their own profiles.

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.

CR data is scheduled and retained in accordance with IRS Records Control Schedule 31, items 24 and 25 (published in Document 12990). Audio and screen captures used for evaluative reviews are deleted from the server after 18 months. Non-evaluated files are deleted no longer than 45 days from the date of the original recording. No PII data is retained by contractors or employees.

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)? In-process

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 7/15/2016

23.1 Describe in detail the system's audit trail. There are several types of audit trails generated in the Ultra software. These provide a record of the actions performed in the various Ultra business and administrative applications, for example who logged into the system, performed a search, played back, etc. Each action is noted in one of the audit trail files and is accompanied by descriptive information of the action. The information is displayed in the following order (delimited by semicolons): ;;;;. The audit trail file is created once a day in the D:\Comverse\Audit Trail\Log folder on the relevant server. The file is created with the *.lrf extension in the following format: Audit Trail_mm.dd.yy_hh.mm.ss.mmm.lrf where: mm.dd.yy= hh.mm.ss.mmm= The hour the file is created is determined by the last time the server, which hosts the audit trail file, was restarted. For example, if you restarted the IntelliFind Application Server at 16:45, the IntelliFind Application Audit Trail file will include all activities performed from 16:45 on the previous day to 16:44 on the day on which it is created. At any point in time, a history of the last 10 audit trail files is available. Each day when a new file is created (the eleventh file in the folder), the oldest of the existing files is deleted. Ultra provides audit trail files for the following applications: • Ultra portal (IntelliQuality, Customer Xperience, Contacts) • Form Fillout (submitting evaluations and assessments) • Form Designer • IntelliMiner Instance Builder • IntelliFind Instance Builder • IntelliFind Application • User Manager • Storage Manager • Reports

J. PRIVACY TESTING

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

24c. If **no**, please explain why. The system functionality is provided by commercial off-the-shelf software. The software inputs and outputs were tested upon implementation but do not require recurring testing.

K. SBU Data Use

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

25a. If **yes**, was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

If **yes**, provide the date the permission was granted.
If **no**, explain why not.

25b. If **yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?
If **no**, explain why not.

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>More than 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
