

NOTE: The following reflects the information entered in the PIAMS website.

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: February 11, 2015

PIA ID Number: **895**

---

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Contact Analytics, CA

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Under 100,000

---

## 4. Responsible Parties:

---

N/A

---

## 5. General Business Purpose of System

---

Contact Analytics (CA) is a program which provides Commercial-off-the-Shelf (COTS) tools for evaluating recorded audio from contact center recordings for the purpose of identifying contact center improvement opportunities. Large segments of recorded messages can be selected as a group, reviewed and compared using user-specified search criteria. The analytic tools provide the capability to drill down to individual recordings to hear selected conversations. Based on criteria provided, the Contact Analytic application will interface with the master recording index maintained by the Contact Recording system which stores information on the location of recorded conversations by agent, call type, handle time, and other metadata. Due process is provided pursuant to 26 USC and 5 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 11/19/2007 12:00:00 AM

---

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies)  
(refer to PIA Training Reference Guide for the list of system changes) No
  - System is undergoing Security Assessment and Authorization No
- 

6c. State any changes that have occurred to the system since the last PIA

None

---

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

---

## B. DATA CATEGORIZATION

---

Authority: OMB M 03-22 & PVR #23- PII Management



---

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

SSN are not used. They are present in CA because of the nature of the audio conversations in Contact Recording.

---

Describe the PII available in the system referred to in question 10 above.

For account-related calls, taxpayer may be required to provide SSN/EIN, name, address, telephone number and DOB. Employee is required to provide name or approved pseudonym and SEID number.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Log-on/password information of analyst/business, systems administrator, quality reviewer

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

---

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

If **Yes**, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: Yes If **Yes**, specify: Contact Recording

---

### C. PURPOSE OF COLLECTION

---

*Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use*

13. What is the business need for the collection of PII in this system? Be specific.

To answer account-related calls, employees must access IDRS/CADE, using their unique log-on and password. Under Restructuring & Reform Act 1998, employees having public contact are required to provide their name or approved pseudonym and unique identification number. To guard against disclosure in account-related calls, taxpayers are required to provide their SSN/EIN, name, address, telephone number and DOB.

---

### D. PII USAGE

---



---

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

19a. If **Yes**, how does the system ensure "due process"?

Yes. Employees will have the opportunity to hear the recording during a feedback session. There will be no effect on the taxpayer.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If **No**, how was consent granted?

Written consent

Website Opt In or Out option

Published System of Records Notice in the Federal Register

Other: Audio message stating calls maybe recorded for quality assurance.

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Yes

\_\_\_\_\_

---

## G. INFORMATION PROTECTIONS

---

*Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures*

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		_____
Contractor System Administrators		<u>Read Only</u>
Contractor Developers		<u>Read Only</u>
Other:	<u>No</u>	_____

If you answered yes to contractors, please answer **22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

Roles and permissions will be developed and the OL5081 process utilized to determine access. The next-higher level of management determines profiles for each analyst and quality reviewer. Upper management and NTEU representatives will have the right to listen to recorded contacts should grievances/disagreement occur regarding content.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

These contacts routinely concern a current tax year. The taxpayer, in the vast majority of cases, has initiated the contact for the dual purpose of securing information from the IRS and providing the IRS with additional information

regarding his/her tax account or situation. Examples – (1) entity updates; (2) ACS histories; (3) closure of an open AUR case (input of TC 290 for \$0.00).

---

25. 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? No

---

25a. 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.

If **No**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

Contact Analytics (CA) is a non-recordkeeping data/audio analysis platform and not the official repository for any evaluative/non-evaluative quality review data. CA examines the audio on the contact recording system, but does not retain it.

---

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.  
Security scans run monthly for vulnerabilities Windows patches are installed regularly Access is managed via OL5081

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.  
The servers are in a locked cabinet within an access controlled data room.

---

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

---

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.  
Security Assessments are performed as a part of FISMA and continuing monitoring activities.

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

---

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

---

## **H. PRIVACY ACT & SYSTEM OF RECORDS**

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

---

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

**SORNS Number**

**SORNS Name**

Treas/IRS 00.009 Recorded Quality Review Records

Treas/IRS 34.037 Audit Trail and Security Records System

**I. ANALYSIS**

*Authority: OMB M 03-22 & PVR #21- Privacy Risk Management*

---

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)

No

Provided viable alternatives to the use of PII within the system

No

New privacy measures have been considered/implemented

Yes

Other:

No

32a. If **Yes** to any of the above, please describe:

Considered what can be done in the next iteration of the product to protect PII.