

Date of Approval: 08/11/2026
Questionnaire Number: 2794

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Cloud Natural Language Interactive Voice Response

Acronym:

CNLIVR

Business Unit

Information Technology

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The IRS Cloud Natural Language (CNL) Interactive Voice Response (IVR) is a modernization effort focused on improving taxpayer & IRS employee's customer service experience. The intent was to migrate certain IRS self-service applications (listed below) from legacy Dual Tone Multi Frequency (DTMF) menu tree system to a conversational IVR Cloud platform. The new platform uses Nuance (vendor) Digital Contact Center Platform (DCCP) that leverages Natural Language Understanding (NLU), Natural Language Processing (NLP), and Artificial Intelligence (AI) technology. DCCP is a Software as a Solution (SaaS) that is managed by Verizon.

The overall project target is to provide automated conversational responses to enable self-service options and reduce the need to contact an agent by allowing a Voicebot to assist the caller (i.e., taxpayer and/or their power of attorney (POA)),

IRS employee). Taxpayer & IRS employee interaction with the IVR will be conversational in nature and streamline access to desired services to speak with an IRS Customer Service Representative (CSR). In addition, successful implementation is expected to improve taxpayer service by lowering the Average Speed to Answer (ASA) and allowing IRS assistors to concentrate on more complex inquiries.

There are six Voicebot applications on the DCCP.

First one is Taxpayer Services Voicebot which includes unauthenticated and authenticated call flows for business owner, Accounts Management (AM). The authenticated call flows include Where's My Refund (WMR), Where's My Amended Return (WMAR), Refund Trace, Transcript, and TAC Appointment. WMR allows taxpayers to obtain the status of their refund and fact of filing information. Taxpayers can initiate a Refund Trace, or re-issuance of their refund check, for their current year refunds. Where's My Amended Refund (WMAR) that allows taxpayers to request the status of their amended tax return. Transcript allows taxpayers to request a transcript be mailed to them without engaging with a CSR/agent. TAC Appointment presents the opportunity for taxpayers to request to cancel or update their appointment, enabling efficient service by eliminating complex IVR menu trees by transitioning to conversational interactions. The second is Automated Collection System (ACS) Voicebot which includes unauthenticated and authenticated call flows for business owner Small Business Self-Employed (SBSE) which allow taxpayers to verify their Location and Transcript, Payoff and View Credit, View Debit, Voice Balance Due (VBD). Financial Relief call flows are unauthenticated and help taxpayers understand and access payment plans, penalty relief, and hardship options like Installment Agreements, Direct Debit Installment Agreements, Currently Not Collectible (CNC) status, and First-Time Penalty Abatement. This bot provides a broader range of financial assistance to help taxpayers resolve outstanding balances and avoid enforcement actions.

The third is Automated Underreporter (AUR) Voicebot with authenticated call flows, for business owner SBSE, to address taxpayer questions regarding AUR topics, i.e., did you get my mail, what's my case status, extension request. The fourth is Insolvency Voicebot with unauthenticated call flows for business owner is SBSE. Assists with general insolvency inquiries, helping taxpayers understand how their balance due impacts bankruptcy cases and what options are available.

The fifth is Specialty Collection Offer In Compromise (SCOIC) Voicebot with unauthenticated call flows for business owner is SBSE. SCOIC voicebot focuses on Offer in Compromise (OIC) eligibility and whether taxpayers qualify for tax debt settlement at a reduced amount.

The sixth is the Information Technology Service Desk (ITSD). IRS employees who call the IT Service Desk for help interact with a voicebot designed to make it easier to get faster resolutions. The automated voicebot will prompt and confirm the caller's SEID, callback number, and location (office or remote). Its integration represents the first step toward delivering fully automated, seamless IT Service Desk support, reducing the need for employees to wait for live agent availability.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

The CNL IVR system processes personally identifiable information (PII) solely for authorized operational purposes related to responding to caller inquiries and providing requested services. The system supports both authenticated and unauthenticated voicebot interactions. Authenticated voicebot interactions request and process PII necessary to fulfill specific service requests that require identity verification, while unauthenticated voicebot interactions do not request PII and are limited to general information or non-sensitive inquiries. This design minimizes PII collection to only when required. PII is collected only when voluntarily provided by callers and is not used for secondary purposes such as profiling, analytics, testing, training, or research. All PII processing performed by CNL IVR is consistent with documented system functionality and applicable IRS privacy policies. The CNL IVR system collects caller-provided personally identifiable information (PII) and transmits the information via a secured interface to the Enterprise API Gateway, which is a component within the GSS-42 boundary. The Enterprise API Gateway forwards the information to the ICCE boundary for downstream processing. The CNL IVR system is designed to accurately capture PII as provided by the caller and to transmit the information without modification or transformation that could affect data quality. Secure transmission mechanisms are used to preserve the integrity of PII in transit. PII processed by CNL IVR is handled transiently in memory and is not stored or retained by the system; upon completion of the call session or transaction, the data is automatically cleared from system memory in accordance with IRS data minimization and retention policies, ensuring timely destruction and reducing the risk of unauthorized access or persistence.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Federal Tax Information (FTI)

Name

Preparer Taxpayer Identification Number (PTIN)

Social Security Number (including masked or last four digits)

Standard Employee Identifier (SEID)

Tax ID Number

Telephone Numbers

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

PII for personnel administration - 5 USC

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system? (Number)

3

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

8037

4.12 What is the previous PCLIA title (system name)?

Cloud Natural Language Interactive Voice Response, CNL IVR

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

The CNL IVR system has undergone a Privacy Threshold Analysis (PTA) in accordance with IRM 10.5.2.2.9 to determine whether it processes, stores, or maintains personally identifiable information (PII). The CNL IVR PCLIA 8037 was processed and approved on 12/20/2023, prior to system deployment. CNL IVR POC was advised to submit a PTA to supersede the original PCLIA; PTA 2298 was processed and approved on 5/21/2025. On 1/15/2026 CNL IVR POC was advised that a new PCLIA is required. PGLD determined that the temporary collection of PII during live voice interactions to respond to caller requests required a PCLIA. CNL IVR processes PII transiently in memory for the purpose of call handling and service delivery and is not retained after the interaction is complete. CNLIVR does not maintain, store, or retrieve PII from a system of records.

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

User and Network Services (UNS), Governance Board (GB)

9 Is this System listed on As-Built-Architecture (ABA)? If the system is not in the ABA, then contact the ABA (<https://ea.web.irs.gov/aba/index.html>) for assistance.

Ys

9.1 What is the ABA ID?

211470

10 Does this system disclose any PII to any third party outside the IRS?

Yes

10.1 Does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

Yes

11.1 Describe the business process and purpose of your Artificial Intelligence (AI) and identify what system(s) or business process(es) this AI supports.

CNL IVR uses AI-based voice recognition to interpret caller speech during inbound voice interactions and support automated call handling. The purpose of the AI is to enable natural-language understanding.

11.2 What is the algorithm or learning method used and what database is training your AI?

The system does not use a trained learning model maintained by the business unit. It functions as a voice recognizer and does not train on IRS data or a separate

training database. The voice recognition capability is provided by the underlying platform/vendor component rather than through IRS-managed model training.

11.3 How is this AI system tested and validated to ensure that the decisions or outputs are reliable (relevant to the input) and performs without biases and drifting? Note: Outputs include, User information, transfer to assistor, reports on dashboard depicting activities.

The evaluation is performed through live call testing, where testers place calls and evaluate whether the system correctly understands the spoken input, routes the call appropriately, and produces the expected response. Validation focuses on functional accuracy of speech recognition and call routing rather than model retraining, since the system is not trained by IRS. Ongoing validation is done by checking that the system continues to recognize caller input correctly and that outputs such as user information display, transfer to assistor, and dashboard activity reports remain accurate.

12 Does this system use cloud computing?

Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

Microsoft Digital Contact Center Platform, F1603087869, Certified 4/29/2020

12.2 Does the CSP allow auditing?

Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

IRS

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

Moderate

13 Does this system/application interact with the public?

Yes

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

No

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

No

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

The taxpayer provides consent by voluntarily choosing to use the system and entering their personally identifiable information (PII) as part of that process.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

Yes. Taxpayers voluntarily provide their information when they choose to use this system. Before providing their information, they are notified of the legal authority to collect it, the purpose for which it will be used, with whom it may be shared, and the effect on their request if they choose not to provide the requested information.

13.4 If information is collected from third-party sources instead of the individual, please explain your decision.

No, the taxpayer or designated representative provides the information.

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

CNL IVR provides notice to individuals prior to the collection of information through audio messaging that directs taxpayers on how to proceed, including the option to speak with an IRS agent. Additional notice, consent, and due process are provided through tax form instructions in accordance with 5 USC, which outline the authority, purpose, and use of collected information. Individuals can decline providing information by choosing not to proceed with options that require PII input within the IVR.

15 Is this system owned and/or operated by a contractor?

Yes

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

Yes

15.2 What PII/SBU data does the subcontractor(s) have access to?

Only authenticated call flows currently rely on the use of PII, including SSN, date of birth, mailing address, tax account information, IP PIN, SEID, name and phone number to securely authenticate callers and route requests to IRS self-service applications.

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

IRS Employees: User - Read Only

Contractor System Administrator: Administrator - Moderate

Contractor Users: Read and Write - Moderate

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

The CNL IVR system does not currently present a formal Privacy Act Statement directly within the IVR interface. Individuals are informed through audio prompts that guide them to available options, including the ability to speak with an IRS agent. Notice, consent, and due process related to the collection and use of personally identifiable information (PII) are provided through IRS tax form instructions and supporting documentation in accordance with 5 USC § 552a(e)(3), and compliance is implied when individuals voluntarily proceed with providing information during the interaction. Individuals can decline providing PII by not proceeding with IVR options that require such information or by selecting alternative service channels.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Under 50,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Under 5,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

More than 1,000,000

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

Not Applicable

22 How is access to SBU/PII determined and by whom?

Vendor users with access to the data received from IRS are United States (U.S.) citizens operating from the U.S. or its territories and have a valid, current background investigation in compliance with FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors or equivalent policies

aligned with FedRAMP High Controls. All IRS users with access to the data received from Nuance are U.S. citizens operating from the U.S. or its territories and have a valid, current IRS background investigation in compliance with FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. Background investigations for all users accessing data under this Agreement will be at a National Agency Check Inquiries (NACI) level or higher. However, any user who is a system or database administrator with privileged access to any server and/or network in which relevant taxpayer data will be stored, processed, or transmitted will have a background investigation level equivalent to a Background Investigation (BI) or higher. Data is processed, not stored - data is masked & not retained in system. This is Software-as-a-Solution.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

Yes

24 Explain any privacy and civil liberties risks related to privacy controls.

CNL IVR presents privacy and civil liberties risks due to the processing of personally identifiable information (PII) during live voice interactions, including potential unauthorized disclosure during transmission and AI-driven voice recognition accuracy. However, these risks are mitigated through strict access controls and security requirements, including ensuring that all vendor and IRS users are U.S. citizens operating within the U.S. or its territories with current background investigations compliant with FIPS 201 (PIV), with privileged users meeting higher investigation standards (Background Investigation level or higher). Additional safeguards include secure transmission protocols, role-based access, controlled interfaces, and centralized monitoring, while the system's design as a Software-as-a-Service ensures that PII is processed transiently in memory, masked, and not retained. These combined technical, administrative, and personnel controls significantly reduce the risk of unauthorized access, misuse, or long-term exposure of sensitive information while maintaining compliance with federal privacy and security requirements.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

The DCCP platform, hosted in Microsoft Azure with reports powered by Power BI, maintains a comprehensive, centralized audit trail utilizing native Azure Monitor and Microsoft Entra ID logging capabilities. This system captures detailed authentication and access events, including those originating from IRS users via our established tenant-to-tenant trust Single Sign-On (SSO). These auditing efforts provide critical access information, specifically capturing and tracking login activities, timestamps, user identities, and access status for all users, including the provided export of privileged user activities from Verizon and

HCL Tech. To limit unauthorized monitoring and protect audit data integrity, access to the logging environment is strictly governed by the principle of least privilege using Azure Role-Based Access Control (RBAC) and FedRamp High protocols. Only explicitly authorized security and administrative personnel can view, monitor, or export these audit logs, which secures the audit trail from unauthorized access or tampering.

27 Does this system use or plan to use SBU data in a non-production environment?
No

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Integrated Customer Communications Environment (ICCE)

Incoming/Outgoing

Both

Transfer Method

IPSEC TUNNEL

Interface Type

IRS Systems, file, or database

Agency Name

Application Programming Interface (API)

Incoming/Outgoing

Both

Agency Agreement

No

Agreement Name

Transfer Method

Application to Application (A2A)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 26.019 - Taxpayer Delinquent Account Files

Describe the IRS use and relevance of this SORN.

Taxpayer Delinquent Account Files is maintained by the Internal Revenue Service (IRS), a federal agency. This SORN is relevant because CNL IVR interfaces with IRS systems that provide taxpayers with delinquent account status and other tax account

information covered by this SORN. Records are retrieved using personal identifiers such as the taxpayer's name, Social Security Number (SSN), Taxpayer Identification Number (TIN), or other account identifiers. PII associated with these records may include the taxpayer's name, address, SSN (including masked or last four digits where applicable), TIN, PTIN, telephone number, SEID (for employees), and tax account information as authorized by the SORN.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Audit Trail and Security Records is maintained by the Internal Revenue Service (IRS). This SORN is relevant because CNL IVR generates and accesses audit and security records that support system monitoring, accountability, incident response, and troubleshooting activities. Records are retrieved using personal identifiers such as employee name, Standard Employee Identifier (SEID), user ID, taxpayer name, Social Security Number (SSN), Taxpayer Identification Number (TIN), Internet Protocol (IP) address, or other system identifiers, as applicable. PII associated with these records may include employee name, SEID, user ID, taxpayer name, SSN (including masked values where applicable), TIN, IP address, audit logs, system access information, and other security event data used to monitor and investigate system activity.

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files

Describe the IRS use and relevance of this SORN.

Covers records related to taxpayer inquiries and responses. Relevant because CNL IVR handles caller interactions and service requests

SORN Number & Name

IRS 24.047 - Audit Underreporter Case Files

Describe the IRS use and relevance of this SORN.

Covers records related to underreporter cases and taxpayer inquiries about those cases. Relevant because CNL IVR supports AUR-related call flows and case status inquiries.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

CNLIVR is used by taxpayers to request refund information, tax transcripts, and fact of filing information.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Public customer service operations records

What is the GRS/RCS Item Number?

GRS 6.5, Item 010

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Records generated from operating a customer call center or service center that provides services to the public, including incoming requests and responses, call recordings used for quality control, complaints, commendations, customer feedback, and satisfaction surveys.

What is the disposition schedule?

General records: Destroy 1 year after resolved or when no longer needed for business use
Call recordings: Retain 3-5 years before destruction

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

031

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems.

Records are used to monitor inappropriate systems access by users.

What is the disposition schedule?

Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

030

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems.

Records are used to monitor inappropriate systems access by users.

What is the disposition schedule?

Temporary. Destroy when business use ceases.

Data Locations

What type of site is this?

Environment

What is the name of the Environment?

Microsoft Azure

What is the sensitivity of the Environment?

Federal Tax Information (FTI)

What is the URL of the item, if applicable?

Microsoft Azure environment supporting CNL IVR does not have a single publicly accessible URL.

Please provide a brief description of the Environment.

The CNL IVR system operates within a Microsoft Azure cloud environment that provides the infrastructure and platform services required to support voicebot functionality, natural language processing, and call routing. The environment enables scalable, secure processing of caller interactions and integrates with IRS backend systems to support authentication and service delivery. Azure services are configured in accordance with FedRAMP and IRS security requirements to ensure confidentiality, integrity, and availability of data processed during IVR interactions.

What are the incoming connections to this Environment?

Incoming connections to the Azure environment include: Inbound telephony/voice traffic from taxpayers and users through the IVR platform (via vendor-managed contact center infrastructure) Caller input data (voice or Dual-Tone Multi-Frequency DTMF) processed by the voicebot for intent recognition and service requests API requests from IRS systems (via secure interfaces such as the Enterprise API Gateway) supporting authentication and data validation All incoming connections are secured using approved

encryption protocols and routed through controlled interfaces to ensure proper validation and protection of data in transit.

What are the outgoing connections from this Environment?

Outgoing connections from the Azure environment include:

Secure transmission of processed request data to IRS backend systems (e.g., via the Enterprise API Gateway and downstream systems such as ICCE) for authentication, account lookup, and service fulfillment.

Response data returned to the IVR system to provide callers with requested information or to facilitate call routing.

Audit and system log data transmitted to centralized logging and monitoring solutions (e.g., Splunk) for reporting.

All outgoing connections are secured using encrypted communication channels and comply with IRS security and privacy requirements to protect sensitive information.