United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Genesys Cloud CX	
Preparer: Gloria Meriweather	**Office:** OMS/OITO/EI/DSSD
Date: December 15, 2025	**Phone:** 202-566-0652
Reason for Submittal: New PIA____ Revised PIA__X__ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

The Genesys Cloud CX is a FedRAMP approved Software as a Service (SaaS) web application hosted on the Amazon Web Services (AWS) platform for enterprise-grade communications, collaboration, and contact center management providing Automated Call Distribution (ACD) and Interactive Voice Response (IVR) services to EPA Enterprise IT Service Desk (EISD) Genesys Cloud CX, built on the Amazon Web Services (AWS) platform utilizing a distributed cloud environment to provide secure access.

EPA Enterprise IT Service Desk (EISD), utilizing the Automated Call Distribution (ACD) and Interactive Voice Response (IVR) services, maintains the reliability and seamless operation of the call while also tracking metrics like response time, time to complete the call with customer, as well as other metrics that allow for EISD to track and measure performance.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The specific legal authority for this collection of information is 5 U.S.C. § 301 "Departmental Regulations", 8 U.S.C § 1101, 1103, 1104, 1201, 1255, 1305, 1360 "Aliens and Nationality"44 U.S.C. § 3101 "Records Management by Federal Agency Heads."

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. A system security plan (SSP) has been completed and it undergone its third-party assessment. An Authorization-to-Operate (ATO) has been granted with an expiration date of November 30, 2028.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information in Genesys Cloud CX is NOT covered by the Paperwork Reduction Act (PRA).

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRAMP approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, the data will be maintained and stored in a cloud. Genesys Cloud CX is a FEDRAMP approved SaaS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The information Genesys Cloud CX captures are the agents' first name, agents last name, callers first name, callers last name, number of agents on queue, service level percentage, number of calls waiting, longest wait time, number of calls abandoned, number of calls answered, number of calls offered, number of calls waiting, number of call backs waiting, number of agents interacting with customers, agent status (e.g., busy, offline, interacting and idle), callers phone number, city and

state of external number, date, start time, interaction type, duration of call, direction of call (e.g., inbound or outbound) and Unique Interaction ID.

2.2 What are the sources of the information and how is the information collected for the system?

Genesys Cloud CX utilizes the applications Web RTC built-in service which automatically collects the information from established calls either from the Enterprise IT Service Desk (EISD) personnel or from the customer and auto populates the data. The service desk agent will verify the data with the customer on the call.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use commercial sources or public available data.

2.4 Discuss how accuracy of the data is ensured.

The Enterprise IT Service Desk service desk verifies the data for accuracy with the customer.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Theirs is always a small risk that data collected by the system is distributed or shared to individuals not approved because of agent error.

Mitigation:

There are technical and logical controls in place. In addition, each user of the system must sign a Rules of Behavior (RoB) and complete the EPA Information Security and Awareness Training (ISAT) and continue to take this training annually.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

There are preventative access controls within the Genesys Cloud CX system that enforces role-based access controls (RBAC). These role-based controls provide separation of duties and limits access to data within the application to only approved designated personnel. The assigning of these roles enhances adherence to the principle of least privilege.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

These access controls are documented in EPA Genesys Cloud CX account management procedures document and in the Genesys Cloud CX Access Control SSP implementation.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, there are no other components with assigned roles and responsibilities.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only the EPA Enterprise IT Service Desk agents, supervisors or application engineers will have access. The appropriate FAR clauses for contractors are included in the contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Retained information will be deleted or destroyed when the Agency determines no longer needed for administrative, legal, audit, or other purposes Genesys Cloud CX retains information in accordance with EPA Records Control Schedule 1012 and 1049.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There is a risk that information may be retained longer than needed.

Mitigation:

Genesys Cloud CX system will adhere to Records Control Schedule 1012(b) and 1049(p) associated with its data.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the

Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No information sharing.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

No information sharing externally.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Not Applicable, no sharing of information.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable, there are no agreements in place.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. There is no external sharing.

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

EPA ensures that the practices stated in the PIA are followed by leveraging training, policies, EPA Rules of Behavior, and auditing and accountability. EPA security specifications require auditing capabilities that logs the activity of each user to reduce the

possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify required audit information by user identification, network terminal identification, date and time. All EPA systems must employ auditing measures and technical safeguards to prevent the misuse of data and Genesys CX Cloud is compliant with EPA policies.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

EPA ensures that the practices stated in this PIA are followed by enforcing or leveraging the mandatory completion of the Information Security and Privacy Awareness training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of improper audit.

Mitigation:

Genesys Cloud CX requires auditing capabilities are in place that log the activity of each user to reduce the possibility of the misuse and/or inappropriate dissemination of information from system.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The information used by the system is strictly for the purpose of accurately verifying the customer for return and follow up on calls, improve customer satisfaction, and to help identify common issues for training and educational purposes.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No__X_. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e., any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

The system is not designed to retrieve information by personal identifiers nor is the purpose of the system to retrieve information.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

Only the information required as a helpdesk is captured by the system to be able to accurately identify the customer and be able to call back or reach the customer is collected. All information is protected from unauthorized access through appropriate administrative, physical (CSP environment), and technical safeguards such as restricting access to unauthorized personnel. User actions are tracked via audit logs to identify audit information by user identification and monitored to detect improper use via weekly audit reviews. This help provide preventative measures and acts as a deterrent to unauthorized activity.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There's a low risk of information misuse.

Mitigation:

All user actions are tracked via audit logs and reviewed weekly to identify audit information by user identification, network terminal identification plus date and time. All EPA systems must employ auditing measures and technical safeguards to prevent the misuse of data.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Little to no risk. Nice inContact System will leverage established EPA procedures for redress and follow procedures that will be implemented.

Mitigation:

I attest as the Agency Privacy Officer that **Genesys Cloud CX** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly

Agency Privacy Officer

Cybersecurity Planning & Risk Mgmt Branch

EPA/OFA