Privacy Impact Assessment for

CXone

Retirement Services

Contact Center as a Service

December 14, 2021

Contact Point
Nicholas Ashenden
Deputy Associate Director
Retirement Services

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The United States Office of Personnel Management's (OPM) Retirement Services' (RS) Retirement Information Office (RIO) Contact Center, in conjunction with the Office of the Chief Information Officer (OCIO), is implementing a new contact center system to support RS's call center. The new system will handle a higher volume of inbound telephone calls and emails, upgrade quality monitoring, and improve reporting metrics and workforce management. This PIA is being conducted because the system will contain personally identifiable information (PII) about federal annuitants, their dependents and survivors.

Overview

The United States Office of Personnel Management's (OPM) Retirement Services' (RS) Retirement Information Office (RIO) Contact Center, in conjunction with the Office of the Chief Information Officer (OCIO), is implementing a new contact center system using cloud-based, multi-channel Commercial Off the Shelf (COTS) software based on "Contact Center as a Service" (CCaaS) technology. The new system will support RS's call center and will handle a higher volume of inbound telephone calls and emails, upgrade quality monitoring, and improve reporting metrics and workforce management over the existing legacy system.

As a result, Federal retirees requesting RS services will be far less likely to receive a busy signal and have an improved call center support experience. The new CCaaS system, using NICE InContact's CXone cloud-based approach, replaces an on-premise Cisco-based system that will be decommissioned once the new system is operational. The CCaaS system will serve as one of the primary systems supporting RS retirement and benefit operations under the Civil Service Retirement System (CSRS) and the Federal Employees Retirement System (FERS).

RS is required to provide customer services to federal retirees, survivors, and their families. There are currently 2.7 million annuitants on the RS annuity roll and that number will continue to grow as the aging federal workforce retires. The RIO is the front-line staff for RS and provides services to customers via telephone and email. The RIO receives requests for a wide range of retirement-related services, including but not limited to requests for change of address, change of banking information, change of tax withholding, Services Online password resets, and verification of annuity payments. In addition, the RIO handles questions regarding federal retirement, health benefits, life insurance and other insurance benefits, as well as serving as the RS primary point of contact for individuals to report the death of an annuitant and request the processing of survivor benefits, if eligible.

RS is migrating from the legacy CISCO-based, on-premise call center infrastructure to a cloud-based system to improve the quality of service to retirees (fewer busy signals, shortened wait-times for RIO support) and to leverage the flexibility of the cloud by surging system infrastructure in times of peak support requests.

The new RS CCaaS system will collect information about current and future retirees including, e.g., name, contact information, address, and other details an individual may relay in their call to the center). RS collects this information in order to provide customer services attendant to the retirement accounts of their customers. The customer service agents that service the RS CCaaS system are Federal customer service specialists in RS.

The following is an overview of the RS activities that will be covered by the new CCaaS:

Telephony: The current telephony platform will be modernized with a transition to a Cloud Based Voice Over IP (VoIP) solution. As RS customers call RIO, incoming calls will be received over the VoIP solution and routed to the appropriate team based on the caller's requested area of service.

Email: The new system will provide a fully automated solution that directly connects Email messages (including formatted email messages) via the Internet through OPM's Office 365 suite. RS customers sending emails will have their emails routed to a queue for the appropriate team to provide a response.

Call Monitoring Solution: RS managers will have dashboards, reports, and recordings to monitor the quality and performance of the team and effectively monitor agent performance and maximize customer satisfaction and end user experience.

Workforce Management Solution: RS managers will be able to forecast volume and scheduling to boost team efficiency across customer response channels in order to improve overall operational efficiency and better manage day-to day contact center (formerly call center) performance.

Knowledge Management: The system will provide a knowledge management capability that serves as an informational database for RS. With this tool, RS will be able to build content that will enable agents to respond more efficiently to customer needs and, in the future, will provide the opportunity for self-service to customers on frequently answered questions.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Civil Service Retirement System (CSRS) is administered pursuant to 5 U.S.C. chapter 83 and the Federal Employee Retirement System (FERS) is administered pursuant to 5 U.S.C. chapter 84. In addition, the following authorities are relevant to the information in ARS: 5 U.S.C. § 3301 and chapters 87, 89 and 90; Pub. L. 83-598, 84-356, 86-724, 94-455, and 106-265; and Executive Order 9397, as amended by Executive Order 13478.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Retirement records are covered by the OPM/CENTRAL 1, Civil Service Retirements and Benefits SORN. Certain records contained in this system may not be retrieved by personal identifier and are, therefore, not subject to the Privacy Act.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

The NICE CXone system is a FedRAMP-approved system. OPM Security is providing an Interim Authority to Test (IATT) while they complete their review of the FedRAMP controls and determine additional security controls needed for the system.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. Emails are maintained pursuant GRS 6.1 and call center calls, including call center recordings, are maintained pursuant to GRS 6.5, Item 010 (customer service operations records).

The actual retirement case files are maintained pursuant to DAA-0478-2017-0001.

1.5. 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.

The information in the system is not covered by the PRA.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The system will collect information about individuals who contact RS via this system, to include name, contact information such as phone number, email and mailing address, and other details an individual may relay when they contact RS. Additionally, the system includes details regarding contact center agents including contact information, their respective skill area, and their availability. Information is captured as part of the screen recordings but not entered and maintained in this system.

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

The information in CCaaS will be obtained directly from the individual annuitant, survivor, or other contact, who provides it via phone call or email. Data in CCaaS originates primarily from the RIO Contact Center customer. RS call center agents use information from the Annuity Roll System (ARS) and the Annuitant Health Benefits Open Season System (AHBOSS) to respond to caller questions, as well as to communicate with insurance carriers as necessary. There is no integration between the RS CCaaS system and ARS and AHBOSS systems, but RS call center agents review data in these systems to support the caller.

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

No. RS CCaaS does not use commercial sources or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

RS call center agents use information in the ARS system to confirm the identity of the caller on the phone.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of collecting extraneous information if customers submit information or attachments in emails to the RIO Contact Center.

Mitigation: This risk will be mitigated by RS call center agents advising users that email correspondence should be limited to the information needed to respond to their support request.

Privacy Risk: There is a risk that the information in customer contact information is not accurate in CCaaS.

Mitigation: This risk is mitigated by the detailed procedures the RIO Contact Center has in place to capture and ensure that the customer information is as accurate as possible during the support call or email exchange. RS call center agents use information in the ARS system to confirm the identity of the caller.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The information in the CCaaS system is used to capture call or email information received by RIO Contact Center agents when responding to a customer request for support. The information is used by agents to manage the call or email communication, and provide information regarding Federal retirement, health, and life insurance benefits.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

No. CCaaS does not use technology to conduct electronic searches, queries, or analyses for the purpose of discovering or locating a predictive pattern or

anomaly. Only data associated with the caller, the caller's, request, and data about the purpose and length of call are captured.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Yes, in addition to RS, the Office of the Chief Information Officer (OCIO) has assigned roles and responsibilities within the system. OCIO will require access for IT support such as installing software on agent desktops in order to access the system and to support administration of the system.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information in the CCaaS system could be used for a purpose other than that for which it was initially collected.

Mitigation: This risk is mitigated by user roles established by the CCaaS Administrator. Only those with a function related to managing the system will be granted access and only authorized users may access or modify the data in the CCaaS.

Privacy Risk: There is a risk that an unauthorized user might access the information in the system or that an authorized user might access the data in the system that he or she does not have a business need to review.

Mitigation: This risk is mitigated through role-based access control and following a strict IT access provisioning policy. Specific roles for Administrators, Managers, and Agents have been defined to prevent unauthorized user access to information

Section 4.0. Notice

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

The individual does not have advance notice from the system, but the RS agent explains to the caller that information will be collected during the call to respond to customer's request for information. In addition, notice about the system is provide via publication of this PIA.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Customers calling into the RS call center are initially advised that their call is being recorded. At that time, customers may opt to exclude themselves by dropping off the call though assistance may be limited if they choose to do so. If customers communicate via email, they may opt to exclude information in email that they do not wish to provide.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not have notice and are not aware that CCaaS contains their information.

Mitigation: This risk is mitigated via publication of this PIA, which provides notice that CCaaS uses and shares data with internal OPM source systems and external Federal agencies for purposes of data matching related to retirement benefits. In addition, RS agents explain to individuals who contact them what information is needed to address the individual's inquiry.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Emails are maintained for seven years pursuant to GRS 6.1; and call center calls, to include screen and voice recordings, are maintained for one year after the issue is resolved (GRS 6.5, Item 010). Recordings are then moved

to archival storage for a period of one year. If an email or details of a call center call need to be maintained longer, those items are converted to a record format (.pdf or word) and maintained in the appropriate file, subject to the retention schedule appropriate to that file. The actual retirement case files are maintained pursuant to DAA-0478-2017-0001.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be kept longer than is necessary to achieve the necessary business purpose.

Mitigation: This risk is mitigated by adhering to the applicable records schedule, which addresses the business need to retain the information. The program office should review the five-year archival of recordings with the Records Officer to determine whether there is a business need to retain those records beyond the one-year base retention called for in the applicable records schedule.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Some of the information in CCaaS may be shared externally with FEHB insurance carriers and other Federal agencies as RIO Contact Center agents work to gather and provide information to customers. Only the information necessary to address the inquiry should be shared.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The information sharing described above is conducted in accordance primarily with the following routine uses in the OPM/CENTRAL 1 SORN.

k. For Non-Federal Personnel--To disclose information to private organizations, contractors, grantees, volunteers, or other non-Federal

personnel performing or working on a project, contract, service, grant, cooperative agreement, or job for, to the benefit of, or consistent with the interests of the Federal Government when OPM has determined that the use of that information is compatible with proper disclosure and will benefit Federal employees, annuitants or their dependents, survivors, and beneficiaries. To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

l. To disclose, to the following recipients, information needed to adjudicate a claim for benefits under OPM's or the recipient's benefits program(s), or information needed to conduct an analytical study of benefits being paid under such programs: Office of Workers' Compensation Programs; Department of Veterans Affairs Pension Benefit Program; Social Security Administration's Old Age, Survivor and Disability Insurance and Medical Programs and Supplemental Security Income Program; Center for Medicare and Medicaid Services; Department of Defense; Railroad Retirement Board; military retired pay programs; Federal civilian employee retirement programs (other than the CSRS or FERS); or other national, State, county, municipal, or other publicly recognized charitable or social security administrative agencies.

m. To disclose to the Office of Federal Employees Group Life Insurance (OFEGLI) information necessary to verify the election, declination, or waiver of regular and/or optional life insurance coverage or eligibility for payment of a claim for life insurance.

n. To disclose to health insurance carriers contracting with OPM to provide a health benefits plan under the FEHB, SSN, and other information necessary to identify enrollment in a plan, to verify eligibility for payment of a claim for health benefits, or to carry out the coordination for benefits provisions of such contracts.

z. To disclose to an allottee, as defined in 5 CFR 831.1501, the name, address, and the amount withheld from an annuitant's benefits, pursuant to 5 CFR 831.1501 et seq. as an allotment to that allottee to implement the program of voluntary allotments authorized by 5 U.S.C. 8345(h) or 8465

bb. To disclose to the Social Security Administration the SSN of civil service annuitants.

6.3. Does the project place limitations on re-dissemination?

No. When information is shared with insurance carriers in order to address an individual's inquiry, the information is shared from ARS (verbally only) and not from the CCaaS system is used.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

hen information is shared with insurance carriers in order to address an individual's inquiry, the information is shared from ARS (verbally only) and not from the CCaaS system is used.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information from CCaaS could be inappropriately disclosed for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by Retirement Center procedures guiding agents to verify an individual's identity so that only callers who are entitled to receive information about an annuitant will receive that information. In addition, agents receive instruction about what external entities it is appropriate to contact and provide information to about an individual caller in order to resolve the caller's inquiry.

Section 7.0. Redress

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

Customers do not have direct access to CCaaS as those records are stored on the NICE CXone system and they will not have access to the system.

Individuals may request access to their retirement records or call center system records by following the instructions in the OPM/CENTRAL 1 SORN and providing the following information: name, including all former names; date of birth; Social Security number; the name and address of the office in which he or she is currently or was formerly employed in the Federal service; and annuity, service credit, or voluntary contributions account number, if assigned. Individuals requesting access must also follow OPM's Privacy Act regulations, 5 C.F.R. part 297, regarding verification of identity and access to records.

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

Customers do not have direct access to CCaaS. Individuals may request that their records be corrected by following the instructions in the OPM/CENTRAL 1 SORN and providing the following information: name, including all former names; date of birth; Social Security number; the name and address of the office in which he or she is currently or was formerly employed in the Federal service; and annuity, service credit, or voluntary contributions account number, if assigned. Individuals requesting access must also follow OPM's Privacy Act regulations, 5 C.F.R. part 297, regarding verification of identity and access to records.

7.3. How does the project notify individuals about the procedures for correcting their information?

Individuals may receive notice by inquiring of RS agents when they make an inquiry about correcting their information. In instances, the PIA and the

OPM/CENTRAL 1 SORN provide information about how to request a correction to records.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be afforded adequate opportunity to correct information in CCaaS.

Mitigation: This risk is mitigated by providing individuals with access to RS agents via the contact center and via the information provided in this PIA and the OPM/CENTRAL-1 SORN.

Privacy Risk: There is a risk that individuals will not be notified concerning their ability to access and amend their records.

Mitigation: This risk is mitigated through publication of this PIA, the OPM/CENTRAL-1 SORN, and via requests of RS agents who can often address an individual's concern.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

CCaaS maintains access roles for OPM personnel and contractors that restrict and grant access to information and functionality based on the user's role in supporting the business process need. CCaaS captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.

OPM personnel review and analyze application records, and review screen and call recordings for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees are required to complete annual IT Security and Privacy Awareness Training. In addition, end-users receive applicable CCaaS content training specific to their work responsibilities, which covers the appropriate use of the information in CCaaS and individual user responsibility.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

CCaaS administrators grant access based on approval from the user's Federal supervisor. Each user is assigned a unique user account and assigned a defined set of privileges based on the least privilege principle. The CCaaS administrator is responsible for ensuring the appropriate authorization has been granted for the access and the privileges requested, and for the removal of the user's privileges once that authorization has ceased.

Since the system is a System as a Service (SaaS) platform, the vendor providing the system provides the same underlying system to multiple customers. The vendor's system employees are responsible for the development, maintenance, and operation of the SaaS platform. The SaaS platform provider does not have direct access to OPM customer data on the system.

RS RIO managers document who has left the contact center each month and the CCaaS administrators will terminate access of any person who leaves OPM employment or who otherwise no longer has a business need that requires access.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

CCaaS does not interface with any other federal systems. There are currently no information sharing agreements or MOUs for the CCaaS system. CCaaS program managers will coordinate with the Office of the Chief Information Officer and with the Chief Privacy Officer, as needed, to review and assess new uses of information contained in CCaaS.

Responsible Officials

Nicholas Ashenden
Deputy Associate Director for Retirement Services

Approval Signature

Signed copy on file with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer