Request for Information

RFI# 02-114-26

State of Alaska
Department of Administration
Division of Retirement and Benefits

Date Issued: March 27, 2026

UNIFIED COMMUNICATION AND COLLABORATION SYSTEM

Introduction:

The State of Alaska, Department of Administration (DOA), Division of Retirement and Benefits (DRB) is seeking information from qualified vendors who are able to provide a Unified Communication and Collaboration (UCC) solution to support DRB's Contact Center queues. The UCC solution must support multiple phone queues, call recording, call log data collection, email integration, and an operator chat function. The system should allow for in-house administration, including configuration of call queues, addition of operators, and management of user access and permissions. Additionally, the system should provide for the collection of call statistics and provide easily accessible and customizable reports on those statistics. Interested parties are requested to provide detailed information about how their UCC solution functions and to describe features and capabilities based on the criteria defined in this RFI.

This request for information (RFI) does not guarantee future work. The information gathered will aid DRB in conducting market research to ascertain the availability and applicability of resources in the marketplace.

Background Information:

DRB is currently using a premise-based interaction client call system that is outdated and no longer meets the division's requirements. The existing system provides multiple call queues, call recording, and operator monitoring; however, it does not allow for modern capabilities such as chat and email integration. The criteria for a potential UCC solution to replace the current call system are outlined below.

Core Criteria:

- Must be a UCC Solution that does not depend solely on the end user having a Microsoft Teams Voice calling plan in order to place outbound or receive inbound calls.
- Must be a direct dial as opposed to utilizing session border controls for function and operation. Vendors may provide justification if their solutions uses a different method and believe it offers advantages.
- Must be a fully developed and widely deployed solution that is not approaching end of life and is expected to remain supported for at least 3-5 years from the date of this RFI.

- If the solution is fully SaaS, vendors must provide a guide or runbook on who is contacted in the event of an outage, degradation in quality, and expected response time for troubleshooting.
- If the solution is fully SaaS, vendors must provide email alerts as to when services, upgrades, updates and patching may take place that could affect the performance of the solution. These updates must not occur during normal operating hours.
- Must include a vendor training plan for administrators, agents, and managers that covers all role-based functions. Training materials should include written documentation as well as recorded training sessions that can be used when onboarding staff.
- Preference is for a cloud hosted (UCaaS) or Hybrid (UCaaS + On-premises) solution.
- Personally identifiable information (PII) data compliant with key regulatory frameworks governing these systems include GDPR, HIPAA, and CCPA, which mandate strict standards for data privacy, storage, and breach notification. Key aspects of PII compliance in UCC:
    - Data Protection Measures: Implementing 256-bit Transport Layer Security (TLS) encryption.
    - Access Controls: Utilizing multi-factor authentication (MFA) and role-based access.
    - Data Loss Prevention (DLP): to monitor and prevent the sharing of PII across chat, video, and email.
    - Voice & Video Compliance: As voice platforms move to the cloud securing voice data—often considered the "weakest link" in compliance—is crucial, requiring solutions that can capture and archive all conversation modalities.
    - Risk Mitigation: Utilizing tools like Session Border Controllers (SBC) helps secure the network edge and regulate traffic.
- Must demonstrate alignment with common regulatory frameworks, which may include GDPR, HIPAA, and/or FedRAMP. As part of their RFI response, vendors must provide governance documentation describing their policies and solution models. This documentation should also include impacts on bring your own device (BYOD) environments if the solution supports or incorporates BYOD functionality.

Core Features:

- The solution should provide a number of standardized reports around queue metrics, individual metrics, and provide a venue for creating customized reports either via PowerBI or a method available within the solution itself.
- Queues and inbound call receiving should use a round-robin method but must also support skill-based routing, allowing those with greater skills to receive inbound calls first.
- Skills should be auditable and editable by users who are identified as managers. This must be separate from company administrators.
- Queues should be easily managed by administrators to include emergency closures, holidays, and special hours where outbound calls are permitted while inbound calls go to voicemail.
- Queues should allow a callback feature for callers who do not want to wait but don’t want to lose their place in the queue.
- Queues should allow agents to place callers on hold and be able to call out to other agents or non-agents for assistance without hanging up on the original caller.
- Queue “on hold” greetings should allow for a combination of music and voice-based notifications.

- Solution should allow text to voice capabilities, should incorporate their own cognitive speech capability or allow integration with Azure Cognitive Services. An available choice of speech styles should be available including male/female voice, accent, etc. if offering as part of the solution.
- Call Center agents (software) must be fully supported under Microsoft Windows 11 Enterprise environments.
- Call Center agents (software) must support standardized USB-A/USB-C headsets with boom mics. Common brands such as Jabra, Plantronics, and Logitech.
- Security Framework should be addressed up front with a "trust but verify" approach.
    - Encryption — In-transit and at-rest, plus meeting and call encryption.
    - Identity & access — SSO, MFA, role-based access, conditional access.
    - Data residency — Where data is stored and how it can be controlled.
    - Compliance frameworks — HIPAA, FINRA, FedRAMP, GDPR, CJIS, etc.
    - Auditability — Logs, retention policies, eDiscovery, legal hold.
- Call logs should be available to designated groups within the UCC solution such as "Supervisors" or "Managers" with the ability to scope relevant staff working under those supervisors or managers.

Additional Features:

- Solution that would be able to be integrated with Azure-based Microsoft Exchange Online.
- Solution that would be able to support Microsoft Teams' integration for collaboration for purposes such as shared workspaces, co-authoring, whiteboarding, and task management.
- Vendors may identify other integration and interoperability features that their solution offers in addition to Microsoft Exchange and Teams.

Response Information:

The purpose of this RFI is to gather information from vendors who are qualified and capable of providing a Unified Communication and Collaboration (UCC) solution for DRB's Contact Center queues.

The Division is seeking information about the types of UCC solutions available in the marketplace as well as the general and benchmark cost of those solutions.

Responses must include the following information:

1. Organization name, contact name, mailing address, phone number, and email of designated point of contact;
2. Description of your existing capability and competence related to the services identified above to include answers to the RFI Questionnaire; and
3. Responses provided in both Word and PDF formats, including any supplemental attachments.

RFI Questionnaire:

The division is interested in the following information as well as any value-added options that your solution offers.

1. What is the name of your organization and your solution?
2. Provide an overview of the ownership of your organization.
3. Provide a general overview of your product and its value proposition (limit to 1,000 words).
4. Provide a general overview of the user experience with your solution.
5. Please provide the general and benchmark cost associated with your program.

6. Please provide your typical implementation timeline for your solution.

This RFI does not extend any rights to prospective vendors or obligate the state to conduct a solicitation or purchase any goods or services. DOA will not award a contract from this RFI, nor will DOA be financially responsible for the preparation, or administration costs incurred to respond to this RFI. All costs associated with responding will be solely at the interested party's expense.

Procurement Officer contact information:

Interested parties must submit a written response by April 13, 2026, at 2:00 p.m. AKST. Responses must be sent via E-mail to doa.oppm.procurement@alaska.gov.

All questions must be in writing and emailed to: doa.oppm.procurement@alaska.gov.
Attention: Taylor Ladner
Department of Administration, Office of Procurement and Property Management

Notice to Vendors:

Pursuant to Administrative Order 352, (a) any person or business determined to support or participate in a boycott of the State of Israel will be disqualified from any procurement related to this Request for Information; and (b) the support of or participation in a boycott of the State of Israel by a person or business contracting with the State of Alaska under AS 36.30 constitutes grounds for termination of the contract.

Administrative Order 352 does not apply to a contract if the person or business has fewer than 10 employees; or the amount to be paid under the contract, excluding renewals and options available under the contract, is less than $100,000.

Disclosure of Submission Contents:

This section governs the ownership, return, and disclosure of any response or other record a Respondent submits in response to this request for information. (Herein, any reference to "Record" includes all such records and the submission response; any reference to "Law" includes any federal or State of Alaska (State) law, including any court or administrative order or rule.)

1. All Records belong to the State.
2. The State has sole discretion regarding whether to return any Record. In exercising this discretion, the State will comply with all Laws.
3. Unless a notice of intent to award is issued pursuant to a subsequent and related solicitation, the State will, to the extent permitted by Law, consider all Records confidential and not subject to the Alaska Public Records Act (APRA).
4. If and when a notice of intent to award is issued, the State will consider nonconfidential any Record unless, at the time of submission, the Respondent undertook the following protective measures:
    a. a. marked information confidential;
    b. b. for any information marked confidential, identified the authority that makes that specific information confidential; and
    c. c. committed, in writing, to explain in detail, including with affidavits and briefs, why each authority applies in any court or administrative proceeding in which any nondisclosure is challenged.
5. If the Respondent did not undertake each protective measure, the State will not consider any information in a Record confidential: the State will disclose the entire Record without any redaction in response to an APRA or other request or, if it chooses, in the absence of a request and the State

will disclose the entire Record without notifying the Respondent.

6. If the Respondent undertook each protective measure, the State will withhold the information marked confidential to the following extent:
    a. a. The State agrees that the Law protects the information; and
    a. b. If the nondisclosure is challenged, the Respondent fulfills its commitment to explain, including with affidavits and briefs, how each authority applies to the information marked confidential.

The State will only notify a Respondent of a request for the Record and of a planned release if the Respondent undertook each protective measure, but the State disagrees that the marked information is protected. If there is such a disagreement, then before releasing the Record, the State will, to the extent permitted by Law and practicable, notify the Respondent that it will disclose the information unless the Respondent convinces the State not to or obtains an order prohibiting disclosure.