



Division of Homeland Security
& Emergency Management
Kevin R. Klein, Director
9195 E. Mineral Avenue, Suite 200
Centennial, CO 80112

MEMORANDUM

Date: October 10, 2013
To: Erin Vanderberg, Colorado Legislative Council
From: Dana Reynolds, Office of Preparedness *D.C. Reynolds*
Subject: Proposed ReadyOP License Sharing Agreement

ReadyOp is a secure web-based application that integrates multiple databases and a communications platform to support planning, response, command and communications for single agencies and unified commands. ReadyOp is designed for fast, efficient access to information, as well as the ability to plan, coordinate, direct and communicate with multiple persons, groups and agencies simultaneously. The Colorado Department of Public Safety (CDPS) endorses this product and is in the process of implementing the solution department-wide to further expand our notification capabilities for both steady-state and crisis-state operations, subject to final approval by the Chief Information Security Officer at OIT. The product is cost-effective, easy to navigate, and equipped with safeguards to ensure continuity during notifications.

The Colorado Legislative Council has requested an initial quote for exclusive use of 25 ReadyOp licenses currently owned by CDPS in a license sharing agreement upon consent of the General Assembly. The per annum cost for these licenses is approximately \$2,500, subject to periodic rate increases initiated by the vendor, Collabria Software. Should the General Assembly wish to partner with CDPS and consent to the license sharing agreement, it is our pleasure to do so. The Legislative Branch will have complete oversight of the 25 user licenses and access rights to the notification platform. One caution is in order, however, with respect to emergency notifications. Because the Executive Security Unit (ESU) of the Colorado State Patrol is charged with ensuring the security of the Capitol complex and any occupants therein, it is paramount that the Legislative Branch coordinate with ESU on the creation and adoption of any emergency notification protocols, especially those that could affect security procedures and protocols already agreed upon and adopted by ESU. To the extent possible, we must avoid duplicative emergency notification procedures being adopted by both ESU and the Legislative Branch as this will only generate confusion during an emergency.

If additional information is needed, please contact me at (720) 852-6634 or via email at dana.reynolds@state.co.us.
We look forward to partnering with the Legislative Branch moving forward.



Division of Homeland Security
& Emergency Management
Kevin R. Klein, Director
9195 E. Mineral Avenue, Suite 200
Centennial, CO 80112

ReadyOp Features

Hosting – ReadyOp uses Amazon Web Services (AWS), an industry leader in secure, reliable cloud computing. Specifically, all US-based ReadyOp clients are hosted through AWS GovCloud. This is a specifically dedicated region of Amazon's Web Services allowing US Government agencies and contractors to move sensitive workloads into the cloud while maintaining regulatory compliance. For US-based clients, ReadyOp's infrastructure is physically and logically addressable by US persons only, supporting the following security controls and certifications: FIPS 140-2, ITAR, HIPAA, FISMA, SSAE 16/SOC1 (formerly SAS-70 Type 2), ISO/IEC 27001, and PCI DSS Level 1. International clients are hosted through the AWS non-US Government secure services.

Secure – Each ReadyOp site is secured using SSL/TLS, the industry standard in secure communications over the Internet. SSL v3, TLS 1.0, 1.1 and 1.2 are used based on the client's browser. This provides the same level of authentication security and encryption of communication, preventing eavesdropping, tampering and forging as required by financial institutions and government regulations for FIPS 140-2 compliance.

Controlled Access Lists - Each agency decides exactly who will have access to its website and the level of interaction authorized for each person. Login access is logged and can be restricted or revoked at any time. The host agency's Agency Administrator and not Collabria gives each person who is granted access the proper credentials.

Agency Administrator - Each agency designates its own Agency Administrator as the control person for that agency. The agency administrator is responsible for maintaining the authorized list of users for his/her agency and for issuing login/security credentials.

Users and Administrators – The agency administrator for each agency designates the persons provided credentials to the agency's site. Users are persons who can log into that agency's ReadyOp site, but a User is not able to see phone numbers or email addresses of persons in the agency's Roster. Administrators can see the contact information, as they are the primary persons responsible for entering and maintaining the personal information for the persons in the Roster.

Chat, Voice, Video – ReadyOp's secure chat feature is encrypted end-to-end using industry standard SSL/TLS. Voice utilizes the SPEEX codec (at ~11kbps), while video uses H.264 (at ~64kbps), allowing audio and video conference calls over even cellular network connections.

Access – Direct access to the ReadyOp software/database is restricted to authorized Collabria personnel only, requiring authentication over private VPN, as well as 4096-bit encrypted authentication.

Backups – All ReadyOp databases are automatically backed up every 4 hours. Backup copies are retained for up to 30 days.

More product information can be found at <http://www.collabriasoftware.com/>