

STATE OF NEW HAMPSHIRE
Dept. of Administrative Services
Div. of Procurement and Support Services
Bureau of Purchase and Property
State House Annex
Concord, New Hampshire 03301

Date: June 29, 2020

NOTICE OF CONTRACT
(Revision)

COMMODITY: VIDEO CONFERENCING SERVICES

CONTRACT NO.: 8002163

NIGP: 915-0000

VENDOR: Interactive Digital Solutions **VENDOR # :** 230762
14701 Cumberland Rd
Suite 400
Noblesville, IN 46060

CONTACT PERSON(S): Gail Szot
Tel. No.: 317-770-3500 ext. 3576 Office, 317-413-2999 cell
E-Mail: Gszot@e-idsolutions.com

EFFECTIVE FROM: July 1, 2017 through June 30, 2021

PRODUCTS & PRICING:

Cost Item	Cost per Item
Monthly Cost per Service Location	\$50.00 /month/location
Cost per Minute	No Charge
Professional Services for Initial Setup (includes all locations, one-time fee)*	\$1495.00 one-time cost
Meeting Room (one-time fee per room)**	\$50.00 one-time cost
Cloud Record 1GB additional cloud recording	\$10.00 per GB
Toll Free Audio	\$20.00 per meeting room per month

PAYMENT: Payments may be made via ACH. Use the following link to enroll with the State Treasury for ACH payments: <https://www.nh.gov/treasury>

INVOICING & PAYMENTS: Invoices shall be submitted after completion of work to the requesting agency. Payment shall be paid in full within thirty (30) days after receipt of invoice and acceptance of the work to the State's satisfaction.

DELIVERY TIME: Within ten (10) working days from placement of order. No minimum order requirements.

SCOPE OF WORK: Contractor shall provide state of the art, quality video conferencing services to all State Agencies by means of a hosted solution. Configuration, management, and support of the video conferencing system and equipment shall be provided by the Contractor. Current Agency configurations shall be duplicated on the new Video Conferencing system. For current agencies, and as new agencies

request services, Contractor shall support equipment selection, installation, configuration, training, maintenance, and support.

Security Requirements

- Health Insurance Portability and Accountability Act (HIPPA) compliance shall be held for the duration of the contract.
- Contractor's system shall be capable of traversing the State's existing networks and abide by respective security policies.

Storage of Data

- Recordings must be stored in a secured, limited access location with off-site redundancy (see HIPPA requirements) – this requirement may be waived during the term of the Contract should DoIT decide to store and take responsibility for recordings locally; Solution shall meet the State of NH security requirements in regards to firewall traversal, encryption of calls, and recording and archiving of calls;
- ANSI/TIA-942 Tier 3 or equivalent Data Center inclusive of redundant equipment and pathways;
- A secure data hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins;
- The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center;
- Contractor shall provide multiple data storage locations, with data stored on secure servers within the United States;
- Contractor shall monitor System, security, and application logs;
- All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs related to the storage of the data or system. Contractor shall allow the State access to system security logs, latency statistics, etc. that affect this Agreement, the State's data or processes. This includes the ability of the State to request a report of the records that a specified user accessed over a specified period of time;
- The Contractor shall monitor physical hardware;
- Contractor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs;
- Back-up copies of State data shall be created for the purpose of facilitating a restore of the data in the event of data loss or System failure or data must be synchronized to another location on a regular basis;
- Contractor shall verify the identity of, or authenticate, all applications, services, users, and processes before allowing use of the System to prevent access to inappropriate or confidential data or services;
- Contractor shall enforce complex passwords for Administrator Accounts of ten (10) characters or more in accordance with DoIT's statewide User Account and Password Policy. This policy is not posted due to security concerns;
- Contractor shall enforce unique user names;
- All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability;
- The Contractor shall execute regular vulnerability scans.

- All solution related devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection;
- All hardware and software components of the Contractor's hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers;
- The Contractor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Contractor's hosting infrastructure and/or the application upon request;
- Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA;
- The Contractor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure;
- The Contractor shall leverage user authentication to provide security and establish permissions. All access shall be through a secure protocol (https), with data encrypted during operation. When the system is at rest there shall be no data exchange.
- Security patching shall be performed as required;
- Data transfer requests must be made in writing and shall be provided through a cloud transfer to a suitable storage location within the United States;
- Contractor shall not access State user accounts or State data except as required to perform the work set forth in this Agreement;
- Contractor shall inform the State of any security breach that jeopardizes the State data. This notice shall be given to the State within 24 hours of its discovery. Full disclosure of the jeopardized data shall be made. In addition, Contractor shall inform the State of the actions it is taking or will take to reduce the risk of further loss to the State;
- In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach;
- Protection of any personal, private and/or sensitive data which may be provided to Contractor as part of this Agreement shall be an integral part of the business activities of the Contractor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, Contractor shall safeguard confidentiality, integrity and availability of the State information and comply with the following conditions:
 - a. Personal information obtained by the Contractor shall become and remain property of the State;
 - b. At no time shall any data or processes which either belongs to or are intended for the use of the State be copied, disclosed, or retained by the Contractor for any party related to the Contractor for subsequent use in any transaction that does not include the State;
 - c. Contractor shall not provide any information collected in the connection with this Agreement for any purpose other than performing its obligations under this Agreement;
 - d. In the event that Contractor stores sensitive personally identifiable information or otherwise confidential information, this data shall be encrypted while at rest or in Motion.
- At the conclusion of the Agreement, either through completion or termination, Contractor shall implement an orderly return of State data in a State defined format at no additional cost to the State. At the State's request, Contractor shall destroy all data in all forms. Data shall be permanently deleted and not recoverable according to National Institute of Standards and Technology approved methods. Contractor shall provide State with certificates of destruction;

Existing Equipment Compatibility

Service must be compatible with existing State videoconferencing equipment located in agencies, Inclusive of:

- Cisco Telepresence system that includes 13 endpoints, Telepresence Management Suite, TMS Scheduler, a VCS Controller and VCS Expressway, a Content Server and a Linux based Telepresence Main Conference Controller;
- Cisco Telepresence SX20 with 12XPHDCAM 1Mic;
- End Point - Profile 52 in w C40 NPP PHD 1080p 12x Cam Touch 2 Mic;
- End Point - Profile 52 Dual w C60 NPP 12x PHD 1080 Cam Touch 4 Mic;
- End Point - Cisco Telepresence MX200 42 PHD 1080p 4x Touch UI Mic;

Authentication and Access Control

- A multi-tenant system that allows accounts to be segmented or integrated according to users or groups shall be supplied. System must define multiple administrators for internal account management;
- System ability to authenticate users using an external LDAP or SAML directory;
- Control shall include three (3) main access roles: administrator, operator and user. Control must support groups to combine users. The administrator shall maintain the system while the operator performs user management.
- Service shall not enforce download license limitations.

Architecture

- Contractor shall use a hot standby configuration to provide redundancy. All servers can be clustered to ensure limitless expandability.
- Service shall be pure-cloud (no hardware required) on-premise hardware/software (no hardware required);

Project Work Plan

Contractor shall perform a site survey and network assessment in order to develop a work plan for the installation of services. Plan shall include each site and anticipated timeframe for service provisioning. Contractor shall provide such plan to the State prior to proceeding with implementations. Project Work Plan and availability shall be completed within thirty (30) days of service request. Plan shall include the following:

- Consultation: appointment/demonstration with State customer. Conduct a needs assessment and discuss potential applications.
- Design: sales and engineering teams work together to design an appropriate solution and deliver a comprehensive solution to the State. Design is subject to review and verification of end user needs.
- Commitment: the customer and Contractor agree to service requirements
- Scope of Work (SOW): the Contractor sales team develops a preliminary overview to finalize Scope of Work (SOW).
- Kickoff: the Contractor team holds a kick off conference call with the customer to review project expectations and to ensure the accuracy of the Statement of Work. The Contractor team and customer shall define and agree on action items for both Contractor and the customer along with target timeframes, logistics and overall process flow.
- Customer Correspondence: the Contractor's project manager assigned to the project shall send project update emails to both the Agency and the internal team on a bi-weekly basis to ensure communication consistency and to help keep project on track. Correspondence by e-mail and phone call shall occur on a daily basis, and include a summary of daily progress, and continue through testing/turn-up to answer any usage questions
- Installation Scheduling: the project manager shall confirm customer availability and readiness for installation can be arranged and installation scheduling can be finalized. Inclusive are

remote configuration and interfacing with the Contractor IT team to ensure sites have the correct network and firewall settings configured.

- Installation and Orientation: Upon completion of remote installation an equipment orientation shall be conducted by the engineer where the customer is familiarized with the solution.
- Project Sign-off: upon successful installation and orientation the State will formally sign-off on the project. (At completion of installation, training and handoff to support team)
- Maintenance Review: the Contractor sales team lead shall contact the customer to review the maintenance initiation and both start and end dates. The Contractor Network Operations Center help desk team shall be introduced to the customer to assist with post-installation inquiries and assistance.
- Satisfaction Survey: the Contractor sales team lead shall review the customer satisfaction questionnaire with customer and establish a submission date for completion. (This happens at project sign-off)
- Constant Contact Policy: the Contractor sales team lead is responsible to ensure that the customer satisfaction continues long after the completion of the install by initiating quarterly communication to inform customer of updates, new offerings and to ensure on-going overall satisfaction. (This is on-going, no less than quarterly)

Functional Requirements

Contractor services shall include the following:

- Video conferences must:
 - Exchange audio and video between two, and up to 100, participants at the same time;
 - Architecture shall allow unlimited conferences simultaneously ;
 - Allow for multiple video views/arrangements (full screen, Hollywood Squares, etc.);
 - Include a "Presenter" view (where audio does not switch away from the presenter);
 - Provide a method of scheduling future conferences through MS Outlook;
 - Provide a method of restricting access to conferences by PIN or passcode login
 - Allow multiple video views/arrangements including full screen, continuous presence and user adjustable (one, two three or more) screens;
 - Presenter view with both fixed and voice activated modes of operation;
 - Content Sharing - ability to share media such as one's desktop computer or individual windows therein;
 - Phonebook/Favorites – to allow users easy access to particular conferences or users;
 - Video Recording by Host- optionally automatic for specific groups;
 - A red recording indicator indicating that recording is on;
 - Unlimited recording.
- Video Streaming Support
 - Support for up to 300 streams for non-members;
 - Administrator dashboard to view storage capacity;
 - Files recorded in MPEG-4/H.264;
 - The ability to download and save recorded files locally;
 - File editing;
 - Video streaming to over 300 individual views from a single stream;
 - Non-browser dependent service;
 - Must be compatible with IE7 and above including Edge and Firefox;
 - Links that can be distributed via e-mail prior to the start of the conference to be streamed;
 - Non-paying members must be able to participate;
 - Phone participation via a local or toll free number.
- Expandability – All agencies within the State of New Hampshire shall be eligible for participation;

Special Requirements for DHHS AAU

- The District office video must be recorded during the entire call (no audio switching to the Hearing Examiner office – this shall not be performed manually.);
- The audio from both the District Office and Hearing Examiner must be recorded;
- District Office dialing per a directory;
- Any Hearing Examiner must be able to dial any other Hearing Examiner unit or District Office unit directly, without being recorded (District Offices do not need this ability);
- Ability to allow only selected participants (Hearing Examiner and District Office participants) and include/exclude participants as needed.

Automated Dashboard

- Online portal dashboard and online account services;
- Administrator level access for State staff using online login;
- Ability to create new hosts/accounts;
- Ability for administrators to view and monitor host activity;
- Ability to retrieve daily usage and other administrative reports on account activity;
- Ability for hosts to view and monitor their use and activity and retrieve billing information;
- Ability for hosts to monitor their conferences online in real time;
- Ability to for hosts to start video conferences from online dashboard;
- Multiple levels of system access;
- Interface for adding, deleting or modifying accounts.
- Facility to view/monitor use and retrieve detailed call records.

Conferencing Features and Functionality

The Contractor shall support the following features and functionality.

- Standards based H.264 and H.323 AVC protocols, and SIP endpoints;
- Perform testing to support of non-standards based methods of conferencing such as Skype for Business, Lync, Canvas and Slack;
- Built-in echo cancellation to ensure the highest quality audio possible;
- Scalable Video Codec (SVC) standard to ensure the highest level of quality possible. This is especially useful in situations where users have limited bandwidth connectivity.;
- Meeting room passcode to prevent unauthorized users from entering a virtual meeting room. Additionally allow a meeting room owner to lock the room after the start of a conference to restrict access.;
- Tools for managing a conference including sending invitations, starting and ending the conference, muting participants, viewing connected participants, muting participants audio and video, disconnecting participants, start and stop recording, sharing data and locking a virtual conference room;
- Host's ability to record conferences.
- Any recorded conference can be played back by a user with the appropriate permissions. They can control the rewind, fast forward, play, pause functions and make full screen.;
- All material used in a recorded conference is automatically included with the recording (website, graphic, document, etc.);
- Support sending automatically generated email and calendar invites;
- Design for mobile use with the number of active users displayed on the screen limited to four. The last users who speak shall show on the mobile device. Android and IOS applications must be available;
- Administrative features to help troubleshoot a failed call including personalized call logs, server alarms, and detailed call records;
- SIP integration to State PBX or Contractor cloud-based VOIP audio service which is offered both as a local and toll-free number;
- User can access system though hard-wired, wireless or 3G/4G connectivity;
- Support of full data sharing by any user; can be application-based or screen-based.;

- Support of both private and public chat from within a conference call.;
- Support a call dashboard that provides complete records for all calls. This includes user, participants, endpoints, call start, end, and duration;
- Call detail information for use in billing and statistics based on the actual usage for several different conference types;
- Tablets and Smartphones Support.

Remote Help Desk and On-Site Support

Remote Help Desk and On-Site Support shall include:

- Contractor assistance to agencies who will need assistance with video endpoint operation and issue resolution;
- Setup of Video Conferencing Service, Endpoints and training staff to use the service/endpoints;
- Ticket management system to track and resolve incidents;
- Support for assisting State Network Engineers to configure SIP/H.323 Registration for firewall/NAT traversal/Port Openings.

Maintenance and Support Services

Vendor shall provide:

- On-site (business hours Monday through Friday, 8:00 a.m. through 4:30 p.m., excluding state holidays) and remote 24x7 tech phone support required with experienced, live technician, capable of troubleshooting and resolving problems encountered;
- Contractor's response to service calls must be within fifteen (15) minutes of submission of request for support;
- Updates and patch management shall be supported by the Contractor;
- Assist State Agencies in the selection of services and video endpoints to meet the needs of the State Agency;
- Ten (10) business days prior notification to the State Project Manager of all changes/updates and State training due to the upgrades and changes;
- Notification of a critical outage designated when a business function cannot be met by a nonperforming application and there is no work around to the problem;
- A record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time;, Implemented I change requests including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close;
- Assistance to the State Network Engineers to configure SIP/H.323 registration for firewall/NAT traversal/Port Openings;
- Assistance to State Agencies in troubleshooting connectivity problems, service quality issues, network configuration and firewall traversal;

Contractor and State Conference

The Account Representative and/or Contractor's Contract Administrator shall meet with State representatives upon request, along with the State's Contract Administrator to evaluate contract implementation and performance and to identify continuous improvement. Frequency of these meetings may be modified with mutual agreement by both parties, or upon demand by the State.

Testing

Contractor shall be called upon to test and assist in the interoperability of any equipment or service provided.

Accessibility Compliance

The State requires ADA compliance for enterprise system solutions. System must be easily adaptable by users with auditory disabilities and those who employ assistive technology to participate in the

video conference experience that is comparable to the experience of users who are not individuals with disabilities.

Management

- Contractor shall provide central management and administrative capabilities including an online portal/dashboard providing advanced management and monitoring capabilities. Dashboard must have multiple levels of system access and provide an easy interface for adding, deleting or modifying accounts. It must also provide a dashboard to view/monitor use and retrieve detailed call records. Dashboard functionality must include origination of email or calendar invitation with a link to join.
- Contractor shall be available for assisting State Network Engineers to configure SIP/H.323 registration for firewall/NAT traversal/Port Openings;
- Contractor shall assist State Agencies in troubleshooting connectivity problems, service quality issues, network configuration and firewall traversal;

Licensing

Contractor shall carry and support all license agreements for the service, as well as any recommended add-ons or extensions. Contractor shall provide copies of license agreements allowing the Contractor to provide or utilize such equipment to the State. Any of the products may be considered at the sole discretion of the State.

QUESTIONS:

Direct any questions to Ryan Aubert, 603-271-0580 or
Ryan.Aubert@das.NH.Gov