INVITATION FOR BID
Managed Information Technology Services

Callaway County Ambulance District is hereby soliciting competitive bids for the above-mentioned services. The successful bidder ("Bidder") will be required to furnish all services note in this specification.

General Bid Information

Bid Title	Managed Information Technology Services
Bid Type	Services
Bid Issued	04/21/2021
Pre-bid Meeting	None
Publication Date	04/21/2021
Bid Due Date	05/07/2021 9:00 a.m.

Instructions for Submitting Bids

Submittal Address	Only electronic submissions will be accepted at info@callawayambulance.org.
Submittal Copies	One (1) pdf document named: Managed Information Technology Services Bid
Submittal Requirements	Bids must include the following in the subject line: Managed Information Technology Services Bid
Late Submittals	Bids received after the time and date stated in the Bid Due Date section will not be considered.

How to Obtain Bid Documents

Location	**Address**
Physical Location	Callaway County Ambulance District 2614 Fairway Drive Fulton, MO 65251 Monday through Friday 9:00 AM to 4:00 PM 573-642-7260 x 24
Internet	

Questions about the Bid or Request for Information

Questions and or Requests for Information (RFI) must be submitted in writing and can be submitted by fax or email as follows:

Primary Contact	Charles Anderson Fax: 573-642-4069 Email: canderson@callawayambulance.org
Questions/RFI Due Date	04/29/2021
Response Date	05/04/2021

Full Opportunity

The District's policy prohibits discrimination or preferential treatment because of race, color, religion, sex, national origin, ancestry, age (over 40), physical or mental disability, cancer-related medical condition, a known genetic pre-disposition to a disease or disorder, veteran status, marital status, or sexual orientation. It is the policy of the Callaway County Ambulance District to encourage and facilitate full and equitable opportunities for small local businesses to participate in its contracts for

the provision of goods and services. It is further the District's policy that no discrimination shall be permitted in small local business participation in District contracts or in the subcontracting of District contracts.

The District reserves the right to reject any or all Bids, to waive any irregularities or informalities not affected by law, to evaluate the Bids submitted and to award the Contract (or Purchase Order) according to the Bid which best serves the interests of the District.

Bid Submission

The submission of a Bid shall be considered conclusive evidence that the Bidder has fully investigated and understands all conditions related to the Bid. The Bidder has read and become familiar with all of the Bid Documents, Attachments, Enclosures, and any Contract or Agreements. No claim for adjustment of the provisions of the Agreement shall be honored on the grounds that the Bidder was not fully informed as to its terms or any of these conditions. No verbal interpretation provided to any Bidder as to the meaning or consequence of any portion of the Bid, the Bid Documents or the Contract or Agreement shall be considered binding on the District. No Bids shall receive consideration by the District unless made in accordance with the following instructions:

1. District's Legal Name and Jurisdiction: The District (District) is legally known as the **Callaway County Ambulance District**. The District is a political subdivision of the State of Missouri. The District has exclusive control and management of all District facilities and property. The District is overseen by an elected board made up of six members. The Director is responsible for the day-to-day operations of the District.
2. Definition of Bidder: The terms "Bidder", "Consultant", "Contractor", "Respondent", "Seller", "Supplier", and "Vendor" whenever appearing in this Invitation for Bid or any attachments, are used interchangeably to refer to the company or firm submitting a Bid in response to this Invitation for Bid.
3. Deadline for Receipt of Bids and Multiple Bids: Bids must be delivered by email to the email address listed in the Invitation to Bid no later than the time specified in the invitation. For the purpose of determining the time a bid is submitted, the District will utilize the date and time the email containing the attachment is received.
4. Requests for Information: Any questions relative to the Bid should be in writing and directed to the designee specified in the Invitation for Bid and by the deadline for receipt of questions.
5. Bid Information: The information contained in this Bid is provided for the convenience of the Bidders. The District does not represent or warrant the accuracy of any financial or statistical information contained in this Bid. In addition, any information contained in any other documents issued by the District, about the District, may only be relied upon by a Bidder at its sole risk. It is the responsibility of the Bidder and other interested parties to assure themselves that the information in this Bid packet is accurate and complete. The District and the Board of Directors, and its employees and advisors, will have no liability arising out of the inaccuracy of any such information.
6. Bid Forms: Bids may be made in a format of the Bidder's choosing, unless otherwise specified. Numbers should be stated in figures and written, and the signatures of all individuals must be in long hand or electronically signed. The completed form should be without interlineations, alterations, or erasures. Discrepancies between multiplication of units of work and unit prices will be resolved in favor of the unit prices. Discrepancies between the indicated sum of any column of numerals and the correct sum thereof will be resolved in favor of the correct sum. In case of conflict between words and numerals, the words shall govern.
7. Execution of Forms: Each Bid must give the full business address of the Bidder and must be signed by the Bidder with his or her usual signature. Bids by partnerships must furnish the full names of all partners and must be signed in the partnership name by a general partner with authority to bind the partnership in such matters. Bids by corporations must be signed with the legal name of the corporation, followed by the signature and designation of the president, secretary, or other person authorized to bind the corporation in this matter. The name of each person signing shall also be typed or printed below the signature. When requested by the District, satisfactory evidence of the authority of the officer signing on behalf of the corporation or partnership shall be furnished. A Bidder's failure to properly sign required forms may result in rejection of the Bid.

Scope of Services

1. Services Included: Bidder agrees to perform Information Technology (IT) managed services (collectively the "Managed Services") for District's devices at the Location(s):
    a. 2614 Fiarway Drive, Fulton, MO 65251
    b. 249 Karen Drive, Holts Summit, MO 65043
    c. 5844 Old US Highway 40, Holts Summit, MO 65262

   For clarification, bidder is only responsible for the Managed Services designated as bidder's responsibility in the table in Appendix A; District is responsible for the items designated as District's responsibility.
2. Service Delivery: All Services will be provided either remotely to District or via scheduled on-site visits to identified District locations. On-site visits that are required beyond the scope of this bid, such as implementations, upgrades, migrations, and/or configuration of new devices will be billed at bidder's hourly rate as determined by bidder, unless otherwise agreed to by the parties. In addition, District agrees to reimburse bidder for any additional expenses and travel costs, including but not limited to transportation, meals and lodging.
3. Security Disclaimer: Bidder may utilize a variety of commercial and in-house developed network scanning tools, vulnerability assessment utilities, penetration-testing tools, and other applications to perform the requirements of the Managed Services. Bidder will perform the Managed Services in such a way as to try to enhance the District's security posture. Since network security is dynamic and constantly evolving, the District acknowledges bidder does not guarantee, and the deployment of the Managed Services will not achieve absolute security or risk elimination for the District. Bidder can only provide reasonable assurances that the Managed Services will endeavor to minimize the amount of exposure to security risk and better prepare the District for a more secure networking environment and does not guarantee that intrusions, compromises, or other unauthorized activity will not occur on District's network or systems. Additionally, bidder is neither responsible for, nor will be held liable for, any system failures due to unforeseen security, configuration, installation anomalies, or the use of recommended software during this process.
4. Hours of Support:
    a. Managed Services, including Remote Help Desk Support, will be provided to District by bidder through remote means between the hours of 8:00 a.m. – 5:00 p.m. Central time Monday through Friday, excluding public holidays.
    b. After-hours emergency support is included for Severity 1* issues only. Any other support issues will be addressed on the next business day during the normal help desk hours set forth above.

   **A Severity 1 issue is defined as a system, or major application or component, going down and no bypass alternative being available, critically impacting District's ability to do business.*
5. Support Tiers:
    a. Bidder will provide the following support tier levels:

Tier	Definition
Tier 1	Tier 1 Support is responsible for filtering Remote Help Desk Support calls and managing the most basic types of service requests and troubleshooting. Activities include: • Basic User Management (e.g., Creating New Users, Resetting Passwords) • Basic Printer Management (e.g., Printer Configuration) • Basic Supported Software Issues (e.g., Common/known issues and general use) • Basic PC Hardware Issues • Basic Networking (e.g., Verifying ISP availability) • Basic Repeatable Processes Defined by "Client Run Book" Tier 1 Support also performs ticket routing and escalation to Tier 2 and Tier 3 support. At maximum, a Tier 1 issue should take no more than 1 hour of support time to resolve. If it exceeds this allotted time with no expectation of resolution by Tier 1 within the next 30 minutes, the support request moves to Tier 2.

Tier 2	Tier 2 Support is responsible for managing more advanced service requests that cannot be resolved by Tier 1 support within an hour. Typically, they are focused on more advanced, but common issues, such as: • Advanced user Issues (e.g., LDAP) • Networking Issues (e.g., NAT, PAT, Access Lists) • Server Hardware Issues (e.g., Common/known issues) • Supported Software Issues (e.g., Requires contacting Vendor) • Basic Security Issues (e.g., Virus or Malware remediation – single device) • Advanced Hardware Issues (e.g., Vendor engagement required) Working off the foundation developed by Tier 1 staff, Tier 2 staff prioritize work based on severity. At maximum, a Tier 2 issue should take no more than 2 hours of support time to resolve. If it exceeds this allotted time, the support request is moved to specialized resource at the Tier 3 level. Tier 2 support maintains ownership of the ticket throughout this process to ensure appropriate District follow-up.
Tier 3	Tier 3 support is responsible for managing highly advanced and typically specialized service requests that cannot be resolved by Tier 2 support within a 2-hour timeframe. Tier 3 support is focused on advanced and uncommon issues, such as: • Advanced Software Issues (e.g., Registry Changes) • Advanced Hardware Issues (e.g., Server, Storage failure/performance diagnosis) • Advanced Networking Issues (e.g., Router, Firewall failure/performance diagnosis) • Advanced Security Issues (e.g., Beyond basis configuration) Dependent on the size, severity, and scope of issues escalated to Tier 3 support requests at this level are resolved as promptly as possible by order of severity. If the support required is complex or will require a separate scope of work, it will result in a billable project being undertaken in accordance with Section 4 below.

Appendix B

Responsibility Section

No.	Responsibility Description	Bidder	District
1	**Technology Management**	**X**	**X**
1.1	**Software**	**X**	**X**
1.1.1	*Servers and Workstations*: Implement fixes on broadly applied software ("Critical Patches"), fixes on known security vulnerabilities ("Security Patches"), and cumulative packages of hotfixes, security patches, critical patches, and other updates ("Service Packs") on a standard monthly cadence. (Microsoft)	**X**	
1.1.2	*Supported Third-Party Applications:* Implement Critical Patches, Security Patches, andService Packs on a standard monthly cadence. *See Appendix D for a full list of covered Third Party Applications as of the Effective Date of this Order*.	**X**	
1.1.3	*Unsupported Third-Party Applications:* District, and not Bidder, will implement Critical Patches, Security Patches, and Service Packs on a standard monthly cadence.		**X**
1.1.4	*Network Device Firmware:* Perform upgrades on a periodic basis.	**X**	
1.1.5	*Virtualization Technology:* Perform Critical Patches and Security Patches for VMWare or Hyper-V on an annual basis. Version upgrades will be performed on an as-requested basis by District.	**X**	
1.1.6	*Inventory:* Create and maintain inventory of all software on the network (Microsoft)	**X**	
1.2	**Remote User Access Control**	**X**	**X**
1.2.1	*Policy Management:* Determine which users are allowed remote access to District Systems. Review access controls annually (at a minimum).		**X**
1.2.2	*User Management:* Provide authorized users access to managed systems via a secure, brokered environment.	**X**	
1.3	**Remote Monitoring**	**X**	
1.3.1	*Remote Basic Monitoring:* 24/7/365 fault monitoring of critical system resources (Memory, disk and CPU utilization). (Service Level Target for critical events: 1-hourresponse during normal business hours; 4-hour response after-hours)	**X**	
1.3.2	*Device Availability/Security:* Ensure devices remain available for general support and monitoring at all hours. (e.g. in order to monitor remotely or patch, the device must remain on and connected to the network.) Ensure physical security of devices		**X**
1.4	**Vulnerability/Security Assessments**		**X**
1.4.1	Assess District's internal network for known vulnerabilities on monthly basis		**X**
1.4.2	Assess up to 16 external IP addresses for known vulnerabilities on an annual basis.		**X**
1.4.3	Monitor exposure of domain name on dark web.		**X**
1.4.4	Conduct quarterly phishing expeditions against District end-users.		**X**
1.4.5	*Pen Test / Red Team Exercises*: Identification of vulnerability on District network from the outside to determine exposure to external threats.		**X**
2	**Network Administration**	**X**	
2.1	**IT Management**	**X**	
2.1.1	*Network Diagram:* Create and update on a quarterly basis a visual diagram of all core infrastructure and edge device connections.	**X**	
2.1.2	*User and System Onboarding:* Document system build procedures for new systems and new users on the network.	**X**	
2.1.3	*Miscellaneous Management:* Document all system information needed to support District (passwords, vendor info, organizational procedures, etc.)	**X**	
2.2	**Network Support**	**X**	

No.	Responsibility Description	Bidder	District
2.2.1	*Technology Checklist:* Complete a quarterly review of District Network Environment (servers, workstations, supported software, backups, antivirus, & power management) against a best practices checklist.	X	
2.2.2	*Remote Basic Monitoring/Alerting/Response:* 24/7/365 fault monitoring of critical network devices and automated alerting. (Service Level Target: 1-hour response during normal business hours; 4-hour response after-hours)	X	
3	**Support Services**	X	X
3.1	**Reactive Support**	X	X
3.1.1	*Remote Help Desk Support:* Provide a centralized access point to District to manage all reactive Tier 1 and Tier 2 support requests.	X	
3.1.2	*On Site Support:* On an as-needed basis, perform onsite support for Tier 1 – Tier 3issues that cannot be resolved remotely or otherwise require physical access to District's systems.	X	
3.1.3	*District Portal:* Provide District with access to online support portal that provides the ability to submit, review, and update service requests. Access granted upon request of District.	X	
3.1.4	*District Availability:* District agrees to make themselves available to assist in troubleshooting or resolving support requests.		X
3.1.5	*Device Availability:* Ensure devices remain available for general support and monitoring at all hours. (e.g. in order to monitor remotely or patch, the device must remain on and connected to the network.)		X
3.1.6	Printers and Other Ancillary Devices: Maintain configuration of physical devices with known best practices based on the findings of ongoing scans and agreed-upon policies and procedures.		X
3.2	**Security Configuration Management**	X	X
3.2.1	User access changes to hardware on the network		X
3.2.2	User changes to software on a system (Microsoft)		X
3.2.3	Encryption of portable devices (verification of supported devices required)		X
3.2.4	Deploy and ensure antivirus tool is up to date	X	
3.2.5	Complete a configuration backup of all network devices pre- / post- major network configuration change	X	
3.2.6	Monitor domain for creation of new users		X
3.3	**Security Log Management**		X
3.3.1	Ensure up-to 5 servers (which will be expressly identified in Exhibit A) are connected to a log management system.		X
3.3.2	Proactive Monitor and analyze logs for identification of anomalies.		X
3.3.3	Proactive reporting of anomalies of concern identified by the log server.		X
3.3.4	Consult and develop Action Plan with District to resolve anomalies identified by the log server.		X
3.3.5	Connect Bidder Network Security Device to District network for the purpose of identifying security risks and system anomalies.		X
3.3.6	Monitor and analyze systems for identification of anomalies as identified by the Bidder Network Security Device.		X
4	**Technology Consulting**	X	X
4.1	**End User Cyber Awareness Training**		X
4.1.1	On-Demand Web-based training focused on cybersecurity topics		X

No.	Responsibility Description	Bidder	District
4.2	**Technology Review**	**X**	**X**
4.2.1	Provide summary ("Technology Summary") of District's technology environment.	**X**	
4.2.2	Participate on a quarterly basis in a review of the Technology Summary between the vCIO and a C-level representative of the District to determine areas for improvementor change.		**X**
4.2.3	Track maintenance contracts on Covered Devices, which are delivered to Bidder by District, informing District in advance of expirations.	**X**	
4.3	**Planning (Annual Plan with Quarterly Activities)**	**X**	**X**
4.3.1	*Architectural Services:* Design new solutions and upgrades to District's existing environment based upon issues identified during Technology Review or upon District request.	**X**	
4.3.2	*Budgetary Planning:* Provide assistance in District's IT Planning and Budgeting processby making recommendations on changes to the environment and providing budgetary quotes for any proposed designs.	**X**	
4.3.3	*Budgetary Planning:* District agrees that at least one C-level individual will participate in all budgetary planning meetings.		**X**
4.4	**Security Policy & Procedure Management**		**X**
4.4.1	Provide recommendations on defined policies and procedures related to IT security.		**X**
4.4.2	Train all employees and ensure adherence to policies and procedures implemented by District based upon Bidder's recommendations.		**X**
5.	**Cloud Services**	**X**	**X**
5.1	**External Protection**	**X**	**X**
5.1.1	*Email Filtering:* Deploy third-party tools for spam, virus, and malware filtering for email via a controlled gateway.	**X**	
5.1.2	*Email Filtering:* District to establish and provide filter rules to Bidder; Bidder responsible to implement rules as directed by District		**X**
5.1.3	*Web Filtering:* Deploy third-party tools for content, virus, and malware filtering for web traffic via a controlled web proxy.	**X**	
5.1.4	*Web Filtering:* District to establish and provide filter rules to Bidder; Bidder responsible to implement rules as directed by District		**X**
5.1.5	*Antivirus:* Deploy a third-party cloud-managed active virus protection tool to all Covered Devices.	**X**	
5.2	**Business Continuity**	**X**	**X**
5.2.1	**Data Backups (Essentials Level of Support)*** • Nightly backups sent to Bidder Datacenter and retained for 30 days** • Ability to restore anything from whole servers to one file • In the event of hardware failure, restoration of server at Bidder Data Center forbusiness continuity*** • Backups monitored daily by Bidder Systems Team • Backup inventory monitored and reported to District by vNA * Backup is for up-to 3 terabytes of data; any additional backup requirements requirean amendment to this Order. **Minimum bandwidth and latency requirements must be met in order to allow for offsite backups. The amount of bandwidth needed will vary based on amount of databeing transmitted. ***1 Month of leasing of Bidder Virtual server free to allow replacement repair of server. Then, standard VM Leasing rates apply.	**X**	

No.	Responsibility Description	Bidder	District
5.2.2	*Disaster Recovery:* In the event of a disaster, temporarily restore business critical systems to Bidder-owned hardware within the Bidder Data Center to include providing remote access to the District via VPN, for up to one month. Restoration to normal productive use is beyond the scope of this Order and will require a separate Order. In addition, disaster recovery for longer than one month is beyond the scope of this Order and will require a separate Order.	**X**	
5.2.3	*Critical Systems:* District to establish a list of critical systems and provide to Bidder for review and approval on a quarterly basis.		**X**
5.2.4	*Waiver of Coverage:* In the event District disregards the written guidance of Bidder in the maintenance or replacement of business-critical systems, District waives their right to all services outlined in this Business Continuity Section.		**X**
5.3	**Hosted Services**	**X**	
5.3.1	*Exchange Email:* Provide an email server, email client, and certain groupware applications.	**X**	
5.3.2	*DNS Services:* Provide third party cloud-based security services tool designed to take steps to protect end users against malware threats they encounter on the internet.	**X**	