STATE OF TENNESSEE
DEPARTMENT OF SAFETY AND HOMELAND SECURITY

REQUEST FOR INFORMATION # 34901-01512 AMENDMENT # 3 FOR RECORDED AUDIO/VIDEO TRANSCRIPTION SOLUTION

DATE: February 9, 2024

RFI # 34901-01512 IS AMENDED AS FOLLOWS:

1. **This RFI Schedule of Events updates and confirms scheduled RFI dates.** Any event, time, or date containing revised or new text is highlighted.

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
1.	RFI Issued		Friday, January 5, 2024
2.	Written Questions and Comments Deadline	2:00 pm	Friday, January 19, 2024
3.	State Responds to Questions and Comments		Friday, February 9, 2024
4.	RFI Response Deadline	2:00 pm	Tuesday, February 27, 2024
5.	Schedule Demonstrations		Tuesday, March 5, 2024
6.	Demonstrations to be Performed in Person or Virtually*.		March 12 -24, 2024

2. **State responses to questions and comments in the table below amend and clarify this RFP.**

   Any restatement of RFI text in the Question/Comment column shall NOT be construed as a change in the actual wording of the RFI document.

Number	Question	Response
1	Do you have a sample output format?	No. An RFI's purpose is to see what is available in the marketplace for services being sought. Please describe the output formats that are offered.
2	How many team members will be using the transcription service?	The State estimates ten to fifteen.
3	What is the average file duration and number of speakers?	The State estimates average file duration anywhere from fifteen minutes to two hours. The number of speakers averages around two to five.
4	Did you have a specific style guide that needs to be followed?	No.
5	Finally, do you have an estimate on the number of files per year?	No.

6	Is this RFI looking for an organization that has already created a product like this and can supply the state with it, or is looking for information on what it would look like to get one created?	The purpose of an RFI is to see what is available. Please explain what your company offers.
7	Who is your current provider(s), if applicable?	We do not currently have a provider.
8	What challenges have you faced from your current vendor(s) on projects with a similar scope of work, if applicable?	N/A
9	What rates are you currently paying for the services requested in this RFI, if applicable?	N/A
10	Is there an Intranet where users will get information about the approved vendor and instructions for accessing services?	No.
11	Are there any additional technologies (if not indicated) that would benefit us to know about?	No.
12	In the Cost Informational Form section, question #3 asks for a rough, non-binding estimated price for the system. Is this question regarding system access only, or the actual transcription services? Because although we do not charge a platform-access fee to access our system, our pricing is based on a per minute model (i.e., the number of audio/video media minutes submitted for transcription). Therefore, we would need an estimate of the total number of minutes the State intends to submit for transcription in order to calculate the total cost. If this number is not known, we can provide the per minute rate, but it will be difficult to determine a total estimated price. Please advise.	See the response to 14.
13	Because we offer many types of transcription services, are we permitted to attach a supplemental, comprehensive pricing proposal in our format outlining all pricing/service options?	Yes, you are permitted to attach your pricing schedule.
14	Is the State open to volume commitments and/or prepayments in order to secure further discounted pricing?	State Procurement Law prohibits from such commitments and/or prepayments.
15	Will the State require English only transcription services, or potential foreign transcription (e.g., Spanish to Spanish) or foreign translation (e.g., English to Spanish)?	The State does not anticipate foreign transcription being needed.
16	Will the transcription services require proper name speaker identification (e.g., Carol Smith)?	No.
17	Will the transcription services require Audio Description (e.g., narrated spoken descriptions of the key visual content)?	No.

18	Is the State interested in human-generated transcription, AI (machine) generated transcription, and/or a hybrid model?	The purpose of an RFI is to see what is available. Please explain what your company offers.
19	Please confirm what security requirements are meant by government cloud standards	Please see the attached document below for the State's standard security requirements. This is subject to change when the formal solicitation is released. Insurance requirements may also be revised. For State language around our requirements for Cloud hosting. Please note we prefer a FedRAMP Moderate environment for State data.
20	Are references required?	This requirement has been removed.
21	What is the current system being used to generate transcripts from audio and video files? a. Is Data Migration from the current system to the new system a requirement? If yes, how much data will be migrated?	The State does not currently have a system used to generate transcripts from audio and video files. a. No.
22	How many total users will be using the new system? a. How many of these users will require administrative or super user privileges? b. How many of these users will require the ability to perform audio and video transcription & export transcripts to make edits? c. How many users would require to simply be able to play audio/video files and view their transcripts?	For total users, please see the response to question 2. a. All of the users would be considered super users. b. All of the users will require the ability to perform these tasks. c. All.
23	How many hours of video and audio will require transcription per month or per year? Can the Department provide some metrics for average frequency of transcription?	1. The State cannot provide a response. 2. No.
24	What is the average length of video and audio file that will require transcription?	Please see response to question 3.
25	What reporting analytics and metrics should the new system be able to generate?	Since this is an RFI, please explain the reporting analytics and metrics that your system is capable of generating.
26	Can you please provide more insight into the Department's support requirements?	Since this is an RFI, please explain the support provided by your company for this product.
27	Does the Department have systems or software that the new solution must integrate with? If yes, please provide more information on the scope of those integrations.	No.
28	Can you please provide more information on the Department's storage requirements?	Since this is an RFI, please explain what storage capabilities provided by your company.

29	Section 5.4-part d states that virtual demonstrations need to be pre-approved by the State. Can you please provide more information on the process of gaining that approval?	Please send your request via email.
30	What is the anticipated RFP release date?	It is unknown at this time. The State typically conducts an RFP over a 6-to-12-month period.
31	Does the Department have a preference for any government cloud vendor for hosting the solution?	The State is comfortable with a SAAS solution hosted in either AWS or AZURE that otherwise meets the requirements of our contract language.
32	How many hours of audio/video do you need transcribed on annual basis?	Please see response to question 5.
33	In our experience, audio and video evidence in a legal matter is organized by cases. Can you provide the number of cases annually from which this material is being generated?	Please see response to question 5.

3. **Delete RFI 34901-01512 Transcription Solution RFI, in its entirety, and replace it with RFI 34901-01512 Transcription Solution V2 attached to this amendment.** Revisions of the original RFP document are emphasized within the new release. Any sentence or paragraph containing revised or new text is highlighted.

4. **RFI Amendment Effective Date.** The revisions set forth herein shall be effective upon release. All other terms and conditions of this RFI not expressly amended herein shall remain in full force and effect.

19. State of Tennessee's Standard Security Requirements:

No Offshore Resources:

Contractor shall limit contractor resources to US-based (onshore) resources only (includes personnel).

Cloud Hosting Statement:

All applications must be hosted in the state's cloud tenant unless an exception has been issued by the STS Security and Risk Management Team

Required Hosting Language:

Contractor Hosted Services Confidential Data, Audit, and Other Requirements

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

(1) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

(2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 or 140-3 (current applicable version) validated encryption technologies. The State shall control all access to encryption keys. The Contractor shall provide installation and maintenance support at no cost to the State.

(3) The Contractor and the Contractor's processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor's and Subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their

control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

(4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

(5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State

(6) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

(1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html.

(2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

(3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

d. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:

(1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:

i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: [NUMBER OF HOURS/MINUTES]

ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: [NUMBER OF HOURS/MINUTES]

(2) The Contractor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

Cyber Insurance:

1) The Contractor shall maintain technology professional liability (errors & omissions)/cyber liability insurance appropriate to the Contractor's profession in an amount not less than ten million dollars ($10,000,000) per occurrence or claim and ten million dollars ($10,000,000) annual aggregate, covering all acts, claims, errors, omissions, negligence, infringement of intellectual property (including copyright, patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, information theft, damage to destruction of or alteration of electronic information, breach of privacy perils, wrongful disclosure and release of private information, collection, or other negligence in the handling of confidential information, and including coverage for related regulatory fines, defenses, and penalties.

2) Such coverage shall include data breach response expenses, in an amount not less than ten million dollars ($10,000,000) and payable whether incurred by the State or Contractor, including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity monitoring or remediation services and expenses in the performance of services for the State or on behalf of the State hereunder.

Personally Identifiable Information.

While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of

PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify or ensure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law. The obligations set forth in this Section shall survive the termination of this Contract.

Confidentiality of Records:

D.34. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.

The obligations set forth in this Section shall survive the termination of this Contract.