STATE OF TENNESSEE
Department of Finance and Administration, Division of TennCare

REQUEST FOR APPLICATION # 31865-00913 AMENDMENT 2 FOR ADVOCACY AND OUTREACH SERVICES DURING THE COVID-19 UNWINDING PERIOD

DATE: February 9, 2023

RFA # 31865-00913 IS AMENDED AS FOLLOWS:

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

EVENT	TIME (Central Time)	DATE (all dates are state business days)
1. RFA Issued		January 20, 2023
2. Written "Questions & Comments" Deadline	2:00 p.m.	January 27, 2023
3. State Response to Written "Questions & Comments"		January 31, 2023
4. Written "Questions & Comments" Deadline (Round 2)	2:00 p.m.	February 16, 2023
5. State Response to Written "Questions & Comments"		February 21, 2023
6. Deadline for Applications	2:00 p.m.	March 6, 2023
7. Evaluation Notice Released		March 13, 2023
8. Effective Start Date of Contract		April 1, 2023

2. Add the following as Sample Grant Section E.15 and renumber any subsequent sections as necessary:

E.15. Grantee 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 Grantee shall protect Confidential State Data as follows:

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

(2) The Grantee shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.

(3) The Grantee and the Grantee'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 Grantee shall provide proof of current ISO certification or

FedRAMP authorization for the Grantee and subcontractor(s), or provide the State with the Grantee's and subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Grantee or subcontractor. The Grantee 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 Grantee 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 Grantee must provide to the State a letter from the Grantee or subcontractor stating whether the Grantee 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 Grantee 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 Grantee 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 Grantee'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 Grantee shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

(5) Upon State request, the Grantee shall provide a copy of all Confidential State Data it holds. The Grantee 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 Grantee 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 Grantee shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

(1) The Grantee and all data centers used by the Grantee 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 Grantee 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, Grantee 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 Grantee 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 Grantee and all subcontractors used by the Grantee. Grantee will maintain and cause its subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Grant Contract. Grantee will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Grantee 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 Grantee'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 Grantee'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 Grantee and subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Grantee 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 Grantee shall maintain set(s) of documents, instructions, and procedures which enable the Grantee 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 Grantee 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: 72-Hours

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: 72-Hours

(2) The Grantee 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 Grantee verifying that the Grantee 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 Grantee shall provide written confirmation to the State after each Disaster Recover Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

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