STATE OF TENNESSEE
Tennessee Bureau of Investigation

REQUEST FOR PROPOSALS # 34800-090422 AMENDMENT # 5 FOR PROVISION OF CLOUD-BASED MESSAGING SWITCH SOFTWARE ON CONTRACTOR-PROVIDED COMPUTING RESOURCES AND MAINTENANCE AND SUPPORT FOR SOFTWARE

DATE: 02/01/23

RFP # 34800-090422 IS AMENDED AS FOLLOWS:

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

EVENT	TIME (central time zone)	DATE
1. RFP Issued		December 19, 2022
2. Disability Accommodation Request Deadline	2:00 p.m.	December 22, 2022
3. Notice of Intent to Respond Deadline	2:00 p.m.	December 29, 2022
4. Written "Questions & Comments" Deadline	2:00 p.m.	January 6, 2023
5. State Response to Written "Questions & Comments"		February 1, 2023
6. Response Deadline	2:00 p.m.	February 10, 2023
7. State Completion of Technical Response Evaluations		February 17, 2023
8. State Opening & Scoring of Cost Proposals	2:00 p.m.	February 20, 2023
9. Negotiations (Optional)		February 21-22, 2023
10. State Notice of Intent to Award Released and RFP Files Opened for Public Inspection	2:00 p.m.	February 23, 2023
11. End of Open File Period		March 2, 2023
12. State sends contract to Contractor for signature		March 3, 2023

13. Contractor Signature Deadline	2:00 p.m.	March 4, 2023

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

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

RFP SECTION	PAGE #	QUESTION / COMMENT	STATE RESPONSE
RFP Section 3.2.2	Pg. 8	1. Would TBI consider electronic submission of the Messaging Switch Software RFP response?	No. The State is requiring one original paper copy and 5 digital copies be mailed to the Solicitation Coordinator prior to response deadline. Please see Item 3 below for additional details.
Schedule of Event Question	N/A	2. Would TBI consider extending the response due date of January 20, 2023?	Please see the schedule above for updated response due date.
RFP Attachment 6.2, Section B: General Qualifications & Experience, Item B.15	Pg. 22	3. B.15 (c) Page 22 of 61 – Estimated Participation Question: If the company is already a WBE owned company AND claims status as a Diversity Business Enterprise under this contract, is there still a requirement to utilize a minority owned business if awarded the contract.	B.15 of the General Qualifications and Experience Items does not require the Respondent to utilize a minority owned business if awarded this contract.
RFP Section 4.8	Pg. 8	4. If responses contain trade secrets and proprietary information, how should this be properly handled and noted in the bid response?	The State does not accept redacted or confidential proposals. Please refer to Section 4.8 of the RFP.
RFP Attachment 6.6, Pro Forma Contract, Term E.7.	Pg. 53-55	5. The Attachment 6.6, Pro Forma Contract, Section E.7 (3) states that the Contractor maintain a Security Management Certification for FedRAMP. Please provide confirmation that this is indeed a requirement for the Contractor of this RFP.	Please see Item 4 below.
General Scope Question	N/A	6. The Contractor shall ensure that the Solution meets all Communication Standards to communicate with NCIC and support one hundred percent (100 %) of all current and future functions of NCIC.	Contractor must ensure that all current and future functions

RFP SECTION	PAGE #	QUESTION / COMMENT	STATE RESPONSE
		COMMENTS: Knowing all future NCIC requirements is tough to ascertain at this time. Most NCIC changes are handled via our maintenance and support contracts, however, some future NCIC requirements may be overarching and additional costs may be involved.	of NCIC are included in the proposed Contract at no additional cost to the State.
RFP Attachment 6.6, Pro Forma Contract, Term A.34.	Pg. 37-38	7. The Contractor shall provide problem management as part of the Maintenance and Support of the Solution. State shall report problem to the Contractor at an agreed upon email address. Critical issues may be reported via phone at an agreed upon phone number or email at an agreed upon email address. a. Problems are divided into three categories and defined, as follows: 06-16-22 FA 6 (1) Critical Problem - a. Problems or issues in the Systems that interrupt or prevent the entire customer population from performing regular business operations; or b. Problems or issues caused by the System having a catastrophic impact defined as disrupting other systems of State or external customers from performing regular business operations. c. Problems in which data may be lost or corrupted (2) Major Problem - a. Problems or issues in the Systems that interrupt or prevent a significant percentage (25% or more) of the customer population from performing regular business operations; or b. Problems or issues caused by the software/service having a major impact on regular business operations by not working in a particular capacity, a slower than normal capacity, or requiring State to troubleshoot with each external customer experiencing the issue. c. Problems where Systems do not work as specified, but there is a simple work-around. d. Problems must be where there is no data loss or corruption. If data loss or corruption, the problem shall be deemed critical. (3) Minor Problem - a. Problems or issues in the Systems that interrupt or prevent an individual from performing regular business operations; b. Problems or issues having a minor impact on regular business operations. Minor impact is defined as System works but optional features are not working properly and the feature does not impact external customers' business needs; c. Information requests; d. Problems involving minor user interface; e. Problems where aspects or features of Systems are missing or failing;	The State declines to amend the problem management language.

<table>
<tr><th>RFP SECTION</th><th>PAGE #</th><th>QUESTION / COMMENT</th><th>STATE RESPONSE</th></tr>
<tr><td></td><td></td><td>f. Problems must be where there is no data loss or corruption. If data loss or corruption, the problem shall be deemed critical.
b. For each of the above Problem types, the following actions must be taken to resolve the Problem as follows (each time period shall be construed as "action completed within XX timeframe"):
Contractor shall follow the following time frames:
Critical Problem: The Contractor shall have an initial response time within fifteen (15) minutes of initial contact from the State. The Contractor shall have a final resolution of incident installed to test within three (3) hours of initial contact from the State.
Major Problem: The Contractor shall have an initial response time within thirty (30) minutes of initial contact from the State. The Contractor shall have a final resolution of incident installed to test within five (5) hours of initial contact from the State.
Minor Problem: The Contractor shall have an initial response time within thirty (30) minutes of initial contact from the State. The Contractor shall have a final resolution of incident installed to test withing one (1) State business day of initial contact from the State.
COMMENTS: CPI provides the following to customers and wishes the above to be comparable.
<table>
<tr><th>Priority</th><th>Description</th><th>Target response time</th><th>Target fix/work around time</th></tr>
<tr><td>Highest</td><td>System failure, Licensee unable to work
Call the Support Center</td><td>Immediate or within 15 minutes to respond to call</td><td>4 hours to resolve or provide a workaround solution</td></tr>
<tr><td></td><td></td><td>1 hour allowed for time to respond</td><td></td></tr>
<tr><td>High</td><td>Software or peripheral failure, Licensee unable to perform some key tasks
Call the Support Center</td><td>Immediate or within 30 minutes to respond to call</td><td>8 hours to resolve or provide a workaround solution</td></tr>
<tr><td></td><td></td><td>2 hours allowed for time to respond</td><td></td></tr>
</table>
</td><td></td></tr>
</table>

RFP SECTION	PAGE #	QUESTION / COMMENT	STATE RESPONSE
		<table><tr><td>Medium</td><td>Intermittent hardware/software problem, Licensee still able to perform key tasks</td><td>Immediate or within 30 minutes to respond to call</td><td>3 working days to resolve or provide a workaround solution</td></tr><tr><td></td><td></td><td>6 working hours allowed for time to respond</td><td></td></tr><tr><td>Low</td><td>Information request, no impact on the Licensee</td><td>Immediate or within 30 minutes to respond to call</td><td>1 working week to provide information or advice</td></tr><tr><td></td><td></td><td>10 working hours allowed for time to respond</td><td></td></tr></table>	
RFP Attachment 6.6, Pro Forma Contract, Term D.33.d	Pg. 51	8. d. Technology Professional Liability (Errors & Omissions)/Cyber Liability 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	The State declines to lower the insurance coverage limits.

RFP SECTION	PAGE #	QUESTION / COMMENT	STATE RESPONSE
		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. COMMENTS: Currently, only $5M of coverage for #2 is available from insurers.	
RFP Section 1.1.2	Pg. 2	9. In section 1.1.2, the RFP states, "The estimated maximum liability is $2,500,000.00." Will the State of Tennessee consider proposals that come in with a total cost higher than $2,500,000.00? Or, will the State treat this total contract liability amount as a mandatory requirement criteria and eliminate any and all proposals that exceed the total contract liability amount of $2,500,000.00?	The State of Tennessee will review and consider all proposals that pass Section A Mandatory requirements.

3. **Delete RFP Section 3.2.2 in its entirety and insert the following in its place** (any sentence or paragraph containing revised or new text is highlighted)**:**

3.2.2. A Respondent must submit original Technical Response and Cost Proposal documents and copies as specified below.

3.2.2.1. One (1) original Technical Response paper document labeled:

"RFP # 34800-092922 TECHNICAL RESPONSE ORIGINAL"

and Five (5) digital copies of the Technical Response each in the form of one (1) digital document in "PDF" format properly recorded on its own otherwise blank, or USB flash drive labeled:

"RFP # 34800-092922 TECHNICAL RESPONSE COPY"
The digital copies should not include copies of sealed customer references, however any other discrepancy between the paper Technical Response document and any digital copies may result in the State rejecting the proposal as non-responsive.

3.2.2.2. One (1) original Cost Proposal paper document labeled:

"RFP # 34800-092922 COST PROPOSAL ORIGINAL"
and one (1) copy in the form of a digital document in "PDF/XLS" format properly recorded on separate, blank, or USB flash drive labeled:

"RFP # 34800-092922 COST PROPOSAL COPY"

In the event of a discrepancy between the original Cost Proposal document and the digital copy, the original, signed document will take precedence.

4. **Delete RFP Section 6.6, ProForma Contract Section E.7. in its entirety and insert the following in its place** (any sentence or paragraph containing revised or new text is highlighted)**:**

E.7. 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 validated encryption technologies.

(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: ONE HOUR

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: FOUR HOURS

(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.

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