STATE OF TENNESSEE
TREASURY DEPARTMENT

DELEGATED AUTHORITY SOLICITATION # 30901-63026 AMENDMENT # 1
For Unclaimed Property Holder and Audit Firms

DATE: July 9, 2025

DLEGATED AUTHORITY SOLICITATION # 30901-63026 IS AMENDED AS FOLLOWS:

1. **This DA Schedule of Events updates and confirms scheduled DA 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. Solicitation Issued		June 9, 2025
2. Notice of Intent to Respond Deadline	2:00 p.m.	June 16, 2025
3. Written "Questions & Comments" Deadline	2:00 p.m.	June 20, 2025
4. State Response to Written "Questions & Comments"		July 9, 2025
5. Offer Deadline	2:00 p.m.	July 18, 2025
6. State Completes Qualifications Evidence Review & Identifies Responsive & Responsible Offers		August 1, 2025
7. State Releases Award Notifications		August 11, 2025
8. Contract Signing		August 15, 2025
9. Contractor Signature Deadline	2:00 p.m.	August 22, 2025

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

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

QUESTION / COMMENT	STATE RESPONSE
1. **Question** SOC 2 Type 2 Examination Requirement Clarification **Solicitation Section:** Pro Forma Contract (Attachment C), Section E. Special Terms and Conditions, Protects and Safeguards Data Provision Number 3 (Solicitation Pages 28-29)	Due to data security concerns, the State will not accept the proposed modification in Question 1. However, in an effort to accept a wider array of vendors while still maintaining a strict level of data security, the State intends to modify the language contained in Section E.3(3), to allow for an SOC 2 TYPE 2, or an ISO 27001:2022 certification.

It is understood that Section E.3(3) requires a SOC 2 Type 2 examination covering Security, Availability, Confidentiality, and Processing Integrity Trust Services Criteria. Given that this solicitation seeks compliance audit services rather than a hosted software platform and/or database, would the State consider the following alternative compliance framework that addresses the same security objectives to satisfy the State's data protection and security requirements: 1. A SOC 1 Type 2 examination (which is the industry standard for audit service providers handling financial data and transactions), AND 2. An ISO 27001:2022 certification covering the Information Security Management System which supports the compliance audit services? This combination would provide: • SOC 1 Type 2: Assurance over controls relevant to financial reporting and audit processes • ISO 27001:2022: Comprehensive coverage of information security controls, including the security, confidentiality, and availability objectives addressed by SOC 2. Would this alternative framework satisfy the State's data protection and security requirements for this audit services engagement?	
2. A6: "Provide a current bank reference indicating that the Offeror's business relationship with its financial institution is in positive standing. Such reference must be written in the form of a standard business letter, signed, and dated within the past three (3) months." A7: "Provide two current positive credit references from vendors with which the Offeror has done business. The references must be written in the form of standard business letters, signed, and dated within the past three (3) months." As the bank is also a vendor, please confirm if it is acceptable to use same letter from the bank to fulfill the requirements for A6 and A7.	If the letter from the bank specifically and clearly addresses both (1) that the Offeror's business relationship with its financial institution is in positive standing and (2) a current positive credit reference, it may be accepted. To be clear, the bank must also be a vendor to the respondent. Specifically, the bank must have provided services to the respondent such as financial advice or loans in exchange for a fee from the respondent. For the bank reference, the respondent must maintain an account with the bank and the bank reference portion must validate the respondent's financial standing and relationship with the bank. Separately, the vendor reference portion must focus on the respondent's payment history with the bank and its creditworthiness.

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

E.3. Protects and Safeguards Data. The Contractor shall protect State Data as follows:

(1) The Contractor shall ensure that all State Data is housed in the continental United States, inclusive of backup data. All State data must remain in the United States, regardless of whether the data is processed, stored, in-transit, or at rest. Access to State data shall be limited to US-based (onshore) resources only.

All system and application administration must be performed in the continental United States. Configuration or development of software and code is permitted outside of the United States. However, software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the U.S. Secretary of Commerce acting pursuant to 15 CFR 7 has defined to include the People's Republic of China, among others are prohibited. Any testing of code outside of the United States must use fake data. A copy of production data may not be transmitted or used outside the United States.

(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 (or 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 any Subcontractor used by the Contractor to host State data, including data center vendors, shall be subject to an annual engagement by a licensed 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") 2 Type 2 examination or shall be in accordance with International Standards Organization ("ISO") 27001:2013. The scope of the SOC 2 Type 2 or ISO 27001:2013 examination engagement must include the Security, Availability, Confidentiality, and Processing Integrity Trust Services Criteria. In addition, the Contractor services that are part of this Contract, including any processing or storage services, must be included in the scope of the SOC 2 Type 2 or ISO 27001:2013 examination engagement(s).

(4) The Contractor must annually review its SOC 2 Type 2 or ISO 27001:2013 examination reports. Within 30 days of receipt of the examination report, or upon request from the State or the Comptroller of the Treasury, the Contractor must provide the State or the Comptroller of the Treasury a non-redacted copy of the Contractor's SOC 2 Type 2 or ISO 27001:2013 examination report(s). The Contractor must review the annual SOC 2 Type 2 or ISO 27001:2013 examination reports for each of its Subcontractors and must also assist the State or Comptroller of the Treasury with obtaining a non-redacted copy of any SOC 2 Type 2 or ISO 27001:2013 examination reports for each of its Subcontractors, including data centers used by the Contractor to host or process State data.

If the Contractor's SOC 2 Type 2 or ISO 27001:2013 examination report includes a modified opinion, meaning that the opinion is qualified, adverse, or disclaimed, the Contractor must share the SOC 2 Type 2 or ISO 27001:2013 report and the Contractor's plan to address the modified opinion with the State or the Comptroller of the Treasury within 30 days of the Contractor's receipt of the SOC 2 Type 2 or ISO 27001:2013 report or upon request from the State or the Comptroller of the Treasury. If any Subcontractor(s) SOC 2 Type 2 or ISO 27001:2013 examination report includes a modified opinion, the Contractor must assist the State or Comptroller of the Treasury with obtaining the Subcontractor(s) SOC 2 Type 2 or ISO 27001:2013 report and the Subcontractor(s) plan to address the modified opinion.

The Contractor must have a process for correcting control deficiencies that were identified in the SOC 2 Type 2 or ISO 27001:2013 examination, including follow-up documentation providing evidence of such corrections. Within 30 days of receipt of the examination report, or upon request from the State or the Comptroller of the Treasury, the Contractor must provide the State or the Comptroller of the Treasury with a corrective action plan and evidence of correcting the control deficiencies. The Contractor must require each of its Subcontractors, including data centers used by the Contractor to host State data, to have a process for correcting control deficiencies identified in their SOC 2 Type 2 or ISO 27001:2013 examination reports and must assist the State or Comptroller of the Treasury with obtaining a corrective action plan and obtaining evidence of correcting control deficiencies identified in Subcontractor(s) SOC 2 Type 2 or ISO 27001:2013 reports.

No additional funding shall be allocated for these examinations as they are included in the Maximum Liability of this Contract.

(5) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment per the NIST 800-115 definition. "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. The Contractor shall provide a letter of attestation on its processing environment that

penetration tests and vulnerability assessments has been performed on an annual basis and taken corrective action to evaluate and address any findings.

In the event of an unauthorized disclosure or unauthorized access to State data, the State Strategic Technology Solutions (STS) Security Incident Response Team (SIRT) must be notified and engaged by calling the State Customer Care Center (CCC) at 615-741-1001. Any such event must be reported by the Contractor within twenty-four (24) hours after the unauthorized disclosure has come to the attention of the Contractor.

(6) If a breach has been confirmed a fully un-modified third-party forensics report must be supplied to the State and through the STS SIRT. This report must include indicators of compromise (IOCs) as well as plan of actions for remediation and restoration. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures.

(7) 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

(8) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy, and ensure all subcontractors 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 always fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

(4) In the event of drive/media failure, if the drive/media is replaced, it remains with the State and it is the State's responsibility to destroy the drive/media, or the Contractor shall provide written confirmation of the sanitization/destruction of data according to NIST 800-88.

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