STATE OF TENNESSEE
DEPARTMENT OF ENVIRONMENT AND CONSERVATION

REQUEST FOR PROPOSALS # 32701-25-414
AMENDMENT # 8
FOR STATE REVOLVING LOAN FUND PROGRAM DATA MANAGEMENT SYSTEM

DATE: March 4, 2026

RFP # 32701-25-414 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		November 17, 2025
2. Disability Accommodation Request Deadline	2:00 p.m.	November 20, 2025
3. Pre-response Conference	10:00 a.m.	November 21, 2025
4. Notice of Intent to Respond Deadline	2:00 p.m.	November 24, 2025
5. Written "Questions & Comments" Deadline	2:00 p.m.	December 3, 2025
6. State Response to Written "Questions & Comments"		December 30, 2025
7. Second Round Written "Questions and Comments" Deadline	2:00 p.m.	March 16, 2026
8. State Response to Second Round Written "Questions and Comments"		March 30, 2026
9. Response Deadline	2:00 p.m.	April 14, 2026
10. State Completion of Technical Response Evaluations		May 8, 2026
11. State Schedules Respondent Oral Presentation		May 12, 2026
10. Respondent Oral Presentation	8 a.m. - 4:30 p.m.	May 14-15, 2026
11. State Opening & Scoring of Cost Proposals	2:00 p.m.	May 18, 2026
12. Negotiation		May 21-22, 2026

13. State Notice of Intent to Award Released and RFP Files Opened for Public Inspection	2:00 p.m.	May 26, 2026
14. End of Protest Period		June 2, 2026
15. State sends contract to Contractor for signature		June 3, 2026
16. Contractor Signature Deadline	2:00 p.m.	June 9, 2026

2. **Delete RFP 32701-25-414 Section 5.1 in its entirety and insert the following in its place** (any sentence or paragraph containing revised or new text is highlighted)**:**

5.1. Evaluation Categories & Maximum Points

The State will consider qualifications, experience, technical approach, and cost in the evaluation of responses and award points in each of the categories detailed below (up to the maximum evaluation points indicated) to each response deemed by the State to be responsive.

EVALUATION CATEGORY	MAXIMUM POINTS POSSIBLE
General Qualifications & Experience (refer to RFP Attachment 6.2., Section B)	**20**
Technical Qualifications, Experience & Approach (refer to RFP Attachment 6.2., Section C)	**30**
Oral Presentation or Field Test (refer to RFP Attachment 6.2., Section D)	**25**
Cost Proposal (refer to RFP Attachment 6.3.)	**25**

3. **Delete RFP 32701-25-414 Attachment 6.2 Section in its entirety and insert the following in its place** (any sentence or paragraph containing revised or new text is highlighted)**:**

RFP ATTACHMENT 6.2. — SECTION C

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION C: TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH. The Respondent must address all items (below) and provide, in sequence, the information and documentation as required (referenced with the associated item references). The Respondent must also detail the response page number for each item in the appropriate space below.

A Proposal Evaluation Team, made up of three or more State employees, will independently evaluate and score the response to each item. Each evaluator will use the following whole number, raw point scale for scoring each item:

0 = little value ***1 = poor*** ***2 = fair*** ***3 = satisfactory*** ***4 = good*** ***5 = excellent***

The Solicitation Coordinator will multiply the Item Score by the associated Evaluation Factor (indicating the relative emphasis of the item in the overall evaluation). The resulting product will be the item's Raw Weighted Score for purposes of calculating the section score as indicated.

RESPONDENT LEGAL ENTITY NAME:	

Response Page # (Respondent completes)	Item Ref.	Section C— Technical Qualifications, Experience & Approach Items	Item Score	Evaluation Factor	Raw Weighted Score
	C.1.	Provide a narrative that illustrates the Respondent's understanding of the State's requirements and project schedule.		**1**	
	C.2.	Provide a narrative that illustrates how the Respondent will complete the scope of services, accomplish required objectives, and meet the State's project schedule.		**4**	
	C.3.	Provide a narrative that illustrates how the Respondent will manage the project, ensure completion of the scope of services, and accomplish required objectives within the State's project schedule.		**4**	
	C.4.	Provide a narrative describing the accessibility and compatibility with common browsers and devices (i.e., Browser, Mobile Web, Mobile Application, tablet, smart device, etc.) offered as part of the solution.		**7**	
	C.5.	Provide a narrative describing the provision of a development, test, and production work environments to support the implementation of the solution.		**7**	
	C.6.	Describe the solution's features and functionality that enables applicant vetting.		**8**	
	C.7.	Provide a description of the solution's method for performing applicant ranking and producing scoring lists.		**8**	
	C.8.	Provide a statement of the features and functionality in the solution that enables access to be granted to external entities for the purpose of viewing submissions and providing scoring input.		**5**	
	C.9.	Describe the extent to which the solution enables internal users' ability to configure and edit application fields and requirements.		**8**	
	C.10.	Provide a narrative to describe the solution's ability to consistently support SRF and SWIG Program workflows. Include details of how the following components can be properly related and tracked: a. Phases: comprised of and driven by various workflow timelines and decision points that drive Statuses, Activities, and Tasks/Actions b. Statuses: driven by initiation, completion, or incompletion of various Activities and Tasks/Actions		**10**	

		c. Activities: driven by initiation, completion, or incompletion of various Tasks/Actions d. Status and Activity combination containing: i. various Documents ii. various rules iii. various notifications iv. various tasks/actions v. timeline restrictions for tasks/actions vi. triggers for manual or automated steps			
	C.11.	As a part of implementation, provide a description of the Respondent's vendor led data migration approach as it relates to: a. data mapping b. data cleansing c. data transformation d. testing		**10**	
	C.12.	Provide a statement describing the Solution's ability to enable and automate workflow events, including communications, notifications, and activity and task functions, that occur phase-by-phase during the SRF program loan process: a. Phase 1 – Questionnaire b. Phase 2 – Financial & Environmental Review c. Phase 3 – Environmental Determination d. Phase 4 – Design Phase e. Phase 5 – Complete Loan Package f. Phase 6 – Managed Projects		**10**	
	C.13	Provide a statement describing the solution's ability to enable and automate workflow events, including communications, notifications, and activity and task functions, that occur phase-by-phase during the SWIG program grant process: a. Phase 1 – Solicitation and Application b. Phase 2 – Evaluation and Determination c. Phase 3 – Grant Award		**10**	
	C.14.	Provide a description of the Respondent's approach to the development of additional phases within the loan and grant workflow process to accommodate program changes.		**8**	
	C.15.	Provide an overview of the solution's ability to trigger alternate progression paths for a submission based on the applicant's ability to satisfy or not satisfy varying loan or grant workflow requirements.		**10**	

	C.16.	Provide an overview of how the solution has been implemented for SRF programs in other states of similar size.		**8**	
	C.17.	Provide a description of the solution’s ability to function as a coordination center for portfolio management activities between the SRF Loan Program and SWIG Program.		**9**	
	C.18.	Provide an overview of the solution’s current or planned cashflow modeling capabilities.		**8**	
	C.19.	Provide a description of the solution’s external customer interface functionality used to facilitate applicant document submissions and data capture.		**10**	
	C.20.	Provide a narrative statement detailing the solution’s data visualization, either native or integrated, intended to drive SRF program analytics.		**10**	
	C.21.	Provide an overview of the solution’s ability to integrate with various systems operating on different technology stacks. Please include: a. Supported integration methods (APIs, file transfers, middleware, etc.) b. Security and compliance considerations for data exchanges c. Any previous experience integrating with state agencies or similar environments		**10**	
	C.22.	Describe the solution’s ability to accommodate one-to-many relationships as it relates to borrowers with multiple business interactions with DWR.		**8**	
	C.23.	Provide a statement to describe the solution’s email tracking capabilities. Include details outlining the solution’s ability to purge emails after they have reached a certain age or met retention requirements.		**7**	
	C.24.	Provide an overview of the document management, file type, and (upload) size accommodations available within the solution. Include details for the following: a. Documentation Management: Accept, process, manage, generate, convert, delete, and securely store print and digital training and certification related documentation. b. Formatting Options: Standard formatting options for uploaded/downloaded, imported/exported, and converted documents and forms including CSV, XLSX, DOCX, JPEG, PNG, HTML, ZIP and PDF.		**7**	

	C.25.	Describe the solution’s ability to enable application submission and support E-sign functionality for applicants.		**7**	
	C.26.	Describe the ad-hoc and user-configurable report capabilities provided within the solution that will support SRF reporting of deliverables to the EPA.		**8**	
	C.27.	Provide a statement describing the solution’s ability to provide SRF program workflow visualization and tracking representations.		**8**	
	C.28.	Describe the solution’s ability to display visual representations of data. Include details for displaying geospatial visualizations and customizable dashboards.		**8**	
	C.29.	Provide an overview of any chatbot and/or wiki help links provided by the solution to provide direction to internal and external customers.		**6**	
	C.30.	Describe the solution’s ability to integrate with the Microsoft (MS) suite including MS Dynamics, MS Outlook calendars and email.		**7**	
	C.31.	Provide detailed information for how the solution will manage and ensure the integrity and security of data audit trails, and history. Specifically, highlight the mechanisms and protocols that will be employed to safeguard the accuracy, completeness, and security of audit logs and historical data including but not limited to individual applications, loans, subrecipient monitoring, and close outs.		**10**	
The Solicitation Coordinator will use this sum and the formula below to calculate the section score. All calculations will use and result in numbers rounded to two (2) places to the right of the decimal point.				**Total Raw Weighted Score:** *(sum of Raw Weighted Scores above)*	
Total Raw Weighted Score **Maximum Possible Raw Weighted Score** *(i.e., 5 x the sum of item weights above)*		**X 30** *(maximum possible score)*		**= SCORE:**	
State Use – Evaluator Identification:					
State Use – Solicitation Coordinator Signature, Printed Name & Date:					

4. **Delete RFP 32701-25-414 Attachment 6.3 in its entirety and insert the following in its place (any sentence or paragraph containing revised or new text is highlighted):**

RFP ATTACHMENT 6.3.

COST PROPOSAL & SCORING GUIDE

NOTICE: THIS COST PROPOSAL MUST BE COMPLETED EXACTLY AS REQUIRED

COST PROPOSAL SCHEDULE— The Cost Proposal, detailed below, shall indicate the proposed price for goods or services defined in the Scope of Services of the RFP Attachment 6.6., *Pro Forma* Contract and for the entire contract period. The Cost Proposal shall remain valid for at least one hundred twenty (120) days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract resulting from this RFP. All monetary amounts shall be in U.S. currency and limited to two (2) places to the right of the decimal point.

ADDITIONAL REQUIREMENTS FOR COMPLETING PROPOSED COST (*I.E.*, MINIMUM AMOUNT, "BLANK" CELLS, *ETC.*)

NOTICE: The Evaluation Factor associated with each cost item is for evaluation purposes only. The evaluation factors do NOT and should NOT be construed as any type of volume guarantee or minimum purchase quantity. The evaluation factors shall NOT create rights, interests, or claims of entitlement in the Respondent.

Notwithstanding the cost items herein, pursuant to the second paragraph of the *Pro Forma* Contract section C.1. (refer to RFP Attachment 6.6.), the State is under no obligation to request work from the Contractor in any specific dollar amounts or to request any work at all from the Contractor during any period of this Contract.

This Cost Proposal must be signed, in the space below, by an individual empowered to bind the Respondent to the provisions of this RFP and any contract awarded pursuant to it. If said individual is not the *President* or *Chief Executive Officer*, this document must attach evidence showing the individual's authority to legally bind the Respondent.

RESPONDENT SIGNATURE:	
PRINTED NAME & TITLE:	
DATE:	
RESPONDENT LEGAL ENTITY NAME:	

Cost Item Description	**Proposed Cost**	**State Use Only**	
		Evaluation Factor	**Evaluation Cost** (cost x factor)
Configuration (as described in pro forma section A.8.)	**$ / COMPONENT**	14	
Integration (as described in pro forma section A.4.)	**$ / SYSTEM**	2	
Migration (as described in pro forma section A.4.)	**$ / SOURCE**	2	
BPI (as described in pro forma section A.9.)	**$ / DELIVERABLE**	1	

RESPONDENT LEGAL ENTITY NAME:			
Cost Item Description	**Proposed Cost**	**State Use Only**	
		Evaluation Factor	**Evaluation Cost** (cost x factor)
Implementation (as described in pro forma section A.4. and A.8)	**$** **/ PHASE**	6	
Training (as described in pro forma section A.5.)	**$** **/ MODULE**	10	
Annual Program Level License (as described in pro forma section A.17	**$** **/ LICENSE**	640	
Annual Hosting and Maintenance (as described in pro forma section A.6 and C.3.)	**$** **/ YEAR**	4	
Solution Support (as described in pro forma section A.6 and C.3.)	**$** **/ HOUR**	1260	
Professional Services (as described in pro forma section A.7, A.9, and C.3.)	**$** **/ HOUR**	20	
Professional services related to change orders (as described in pro forma section A.11)	**$** **/ HOUR**	200	
EVALUATION COST AMOUNT (sum of evaluation costs above)**:** The Solicitation Coordinator will use this sum and the formula below to calculate the Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.			
lowest evaluation cost amount from all proposals **evaluation cost amount being evaluated**	**x 25** **(maximum section score)**	**=** **SCORE:**	
State Use – Solicitation Coordinator Signature, Printed Name & Date:			

5. Delete RFP 32701-25-414 Attachment 6.5 in its entirety and insert the following in its place (any sentence or paragraph containing revised or new text is highlighted):

RFP ATTACHMENT 6.5.

SCORE SUMMARY MATRIX

	RESPONDENT NAME		*RESPONDENT NAME*		*RESPONDENT NAME*	
GENERAL QUALIFICATIONS & EXPERIENCE **(maximum: 20)**						
EVALUATOR NAME						

EVALUATOR NAME						
REPEAT AS NECESSARY						
	AVERAGE:		**AVERAGE:**		**AVERAGE:**	
TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH **(maximum: 30)**						
EVALUATOR NAME						
EVALUATOR NAME						
REPEAT AS NECESSARY						
	AVERAGE:		**AVERAGE:**		**AVERAGE:**	
ORAL PRESENTATION/ FIELD TEST **(maximum: 25)**						
EVALUATOR NAME						
EVALUATOR NAME						
REPEAT AS NECESSARY						
	AVERAGE:		**AVERAGE:**		**AVERAGE:**	
COST PROPOSAL **(maximum: 25)**	**SCORE:**		**SCORE:**		**SCORE:**	
TOTAL RESPONSE EVALUATION SCORE: **(maximum: 100)**						
Solicitation Coordinator Signature, Printed Name & Date:						

6. **Insert the following to RFP 32701-25-414 Attachment 6.6 to create Section D.38 and delete Attachment 6.6 Section E.5 in its entirety** (any sentence or paragraph containing revised or new text is highlighted)**:**

D.38. Information Technology Security Requirements (State Data, Audit, and Other Requirements).

a. "State Data" is any and all data that can be accessed, processed, generated, including derivative works, stored, or hosted by the Contractor in performance of this Contract." 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 C.F.R. § 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 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 shall maintain, obtain, or undergo the following third-party information security **[TBD from RFP proposal: certification(s), authorization(s), examination(s), assessments, or audit(s)]** for both the Contractor and the Contractor's processing environment containing State Data. The Contractor shall ensure that **[TBD from RFP proposal: each certification, authorization, examination, or assessment]** remains current and valid throughout the term of the Contract.

[TBD on the Contractor's proposal that identifies at least one of the following options for insertion into D.38.a.(3) above paragraph and the corresponding paragraph provided below.]

i. **ISO/IEC 27001:2022 Certification** – The Contractor and Contractor's processing environment containing State Data shall be currently compliant with the most recent version of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27001:2022 standards. Annual surveillance and recertification audits shall be performed by a certification body accredited by the ANSI-ASQ National Accreditation Board (ANAB);

ii. **FedRAMP Authorization** - The Contractor and Contractor's processing environment containing State Data shall maintain an active Federal Risk and Authorization Management Program (FedRAMP) Moderate or higher Authorization to Operate as issued by a federal agency or the FedRAMP Program Management Office;

iii. **GovRAMP Authorization** - The Contractor and Contractor's processing environment containing State Data shall maintain authorization by the Government Risk and Authorization Management Program (GovRAMP) and undergo an annual audit performed by a GovRAMP-approved Third Party Assessment Organization (3PAO);

iv. **SOC 2 Type II Examination** - The Contractor and Contractor's processing environment containing State Data shall 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 examination that includes the Security, Availability, and Confidentiality Trust Services Criteria;

v. HITRUST Certification - The Contractor and Contractor's processing environment containing State Data shall maintain a current HITRUST risk-based 2-year (r2) validated assessment issued under the HITRUST Common Security Framework and performed by an authorized HITRUST External Assessor Organization; or

vi. NIST Audit - The Contractor and Contractor's processing environment containing State Data shall undergo an annual independent audit assessing compliance with the privacy and security controls established in the National Institute of Standards and Technology (NIST) Special Publication 800-53. The audit shall be conducted by a qualified independent assessor, which may include a reputable CPA firm, cybersecurity firm, or other organization with demonstrated expertise in assessing NIST control compliance. The audit must evaluate compliance with the security controls defined in the NIST Special Publication 800-53B moderate-impact security control baseline or a higher-impact baseline.

(4) Upon request by the State or the Comptroller of the Treasury, and within thirty (30) days of completion or receipt of [TBD from RFP proposal: any certification, authorization, examination, assessment, or audit] required under Contract Section D.38.a.(3) the Contractor shall provide the State or the Comptroller of the Treasury with the following documentation and deliverables. The Contractor shall ensure that all documentation remains current, complete, and accurate throughout the term of the Contract.

[TBD on the Contractor's proposal that identifies at least one of the following options for insertion into D.38.a.(4) above paragraph and the corresponding paragraph provided below.]

i. ISO/IEC 27001:2002 Certification

1) The ISO/IEC 27001:2022 assessment report in its entirety;
2) The certification letter issued by the accredited certification body;
3) The Statement of Applicability (SOA) in its entirety, including specific clauses, control categories, control objectives, and implemented controls;
4) A written disclosure and rationale for all controls listed as "excluded" in the SOA; and
5) Evidence that annual surveillance and recertification audits were performed by a certification body accredited by the ANSI-ASQ National Accreditation Board.

ii. FedRAMP Authorization

1) The FedRAMP Authorization Letter (Authorization to Operate);
2) The System Security Plan in its entirety;
3) The Security Assessment Plan;
4) The Security Assessment Report in its entirety prepared by the FedRAMP-approved Third-Party Assessment Organization; and
5) The current Plan of Action and Milestones documenting all known control weaknesses and remediation status, which the Contractor shall maintain or cause to maintain in a current and accurate state throughout the term of the Contract.

iii. GovRAMP Authorization

1) The GovRAMP Authorization Letter or equivalent documentation issued by the GovRAMP Program Office;
2) The System Security Plan in its entirety;
3) The Security Assessment Plan;
4) The Security Assessment Report in its entirety prepared by the GovRAMP-approved Third-Party Assessment Organization; and
5) The current Plan of Action and Milestones documenting all known control weaknesses and remediation status, which the Contractor shall maintain or cause to maintain in a current and accurate state throughout the term of the Contract.

iv. SOC 2 Type II Examination

1) The SOC 2 Type II examination report in its entirety;
2) A corrective action plan describing each identified deficiency, planned remediation steps, and anticipated completion dates; and
3) If any SOC examination report for the Contractor or any Subcontractor supporting this Contract includes a modified opinion, meaning the opinion is qualified, adverse, or disclaimed, the Contractor shall notify the State of the modified opinion within thirty (30) days of receipt and provide the Contractor's plan of corrective action.

v. HITRUST Certification

1) The current HITRUST assessment report in its entirety;
2) The HITRUST Certification Letter for the current [r2] Validated Assessment, issued by HITRUST Alliance after validation by an Authorized HITRUST External Assessor Organization, the letter must show assessment type, scope, and certification dates; and
3) A corrective action plan describing each identified deficiency, planned remediation steps, and anticipated completion dates.

vi. NIST Audit

1) The audit report in its entirety;
2) A corrective action plan describing each identified deficiency, planned remediation steps, and anticipated completion dates.

Upon request by the State or the Comptroller of the Treasury, the Contractor shall also provide current Subcontractor certifications, reports, and related deliverables pertaining to services provided under this Contract within thirty (30) days. If any certification, authorization, examination, or assessment required under this Contract for any Subcontractor supporting this Contract lapses, expires, is suspended, or is revoked, the Contractor shall notify the State in writing within five (5) business days of learning of the status change and provide: (i) the effective date and reason; (ii) the services and State Data affected; and (iii) the Contractor's corrective action plan and interim risk mitigations.

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 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 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 shall implement and maintain privacy and security controls that follow the guidelines set forth in NIST 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” as amended from time to time. The Contractor shall meet annually, or as otherwise agreed, with the State to review the implementation of this Section. 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 System Security Plan that describes how the Contractor implemented privacy and security controls within NIST 800-53.

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.

c. Comptroller Audit Requirements.

Upon reasonable notice and at any reasonable time, the Contractor agrees to allow the Comptroller of the Treasury, or the Comptroller’s duly appointed representatives, to perform information technology control audits of the Contractor’s information technology hosting and processing environment used by the Contractor to provide services under this Contract. The audit may evaluate whether the Contractor has implemented appropriate privacy and security controls consistent with NIST Special Publication 800-53, including controls generally classified as general controls and application controls. The audit may also assess whether those controls are designed and operating effectively and whether the Contractor is complying with applicable policies, laws, and regulations.

For purposes of this section:

General Controls are policies, procedures, and technical mechanisms that support the overall operation and integrity of information systems and applications, including areas such as access security, change management, system development, backup and recovery, and system maintenance.

Application Controls are the automated or manual controls built into specific applications to ensure the completeness, accuracy, authorization, and validity of data and transactions processed by those applications.

The audit may include, but is not limited to:

1) Review and evaluation of independent assurance deliverables required under Contract Section D.38.a.(4) to determine whether the Contractor’s or Subcontractor’s control environment and related safeguards are designed and operating effectively;
2) Review of documentation describing the Contractor’s information technology control environment, policies, and procedures;
3) Interviews with technical and management personnel responsible for implementing, monitoring, and maintaining information technology controls;
4) Inspection of technical, administrative, or physical controls implemented to protect State Data and support service delivery under this Contract;
5) Review of relevant transaction logs, audit trails, vulnerability scans, or other supporting evidence necessary to verify compliance with applicable control requirements; and
6) Performance of other audit procedures deemed necessary by the Comptroller of the Treasury to verify compliance with applicable federal or state laws, regulations, or policies, or to assess the adequacy and effectiveness of the Contractor’s control environment.

The Contractor shall ensure that its Subcontractors cooperate and provide reasonable access to information or personnel necessary for the audit to the extent such information pertains to the services provided under this Contract.

The Contractor must have a process for correcting control deficiencies that were identified in the Comptroller of the Treasury's information technology audit. For any audit issues identified, the Contractor shall submit a corrective action plan to the Comptroller of the Treasury which addresses the actions taken, or to be taken, and the anticipated completion date in response to each of the audit issues and related recommendations of the Comptroller of the Treasury. The corrective action plan shall be provided to the Comptroller of the Treasury upon request from the Comptroller of the Treasury and within 30 days from the issuance of the audit report or communication of the audit issues and recommendations. Upon request from the Comptroller of the Treasury, the Contractor shall provide documentation and evidence that the audit issues were corrected.

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:

      Four (4) 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:

      Twenty-four (24) hours

2. The Contractor and the Subcontractor(s) shall maintain a documented Disaster Recovery plan and shall share this document with the State when requested. 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.

7. **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.