STATE OF TENNESSEE
Tennessee Department of Agriculture

REQUEST FOR QUALIFICATIONS # 32505-00215 AMENDMENT # 3 FOR TDA LICENSE, INSPECTION, CERTIFICATION SOFTWARE, SERVICES, AND HOSTING

DATE: 8/11/2015

RFQ # 32505-00215 IS AMENDED AS FOLLOWS:

1. **This RFQ 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 (all dates are State business days)
1.	RFQ Issued		July 17, 2015
2.	Disability Accommodation Request Deadline	2:00 p.m.	July 22, 2015
3.	Notice of Intent to Respond Deadline	2:00 p.m.	July 24, 2015
4.	Written "Questions & Comments" Deadline	2:00 p.m.	July 31, 2015
5.	State response to written "Questions & Comments"		August 11, 2015
6.	RFQ Response Deadline	9:00 a.m.	August 25, 2015
7.	State Notice of Qualified Respondents Released		September 1, 2015
8.	State Schedules respondent Oral Presentations (Only for Qualified Respondents)		September 2, 2015
9.	Respondent Oral Presentations	8:00 a.m. – 4:30 p.m.	September 10-14, 2015
10.	RFQ Cost Negotiations		September 15-16, 2015
11.	State Evaluation Notice Released		September 17, 2015
12.	Solicitation Files Opened for Public Inspection		September 17, 2015
13.	End of Open File Period		September 24, 2015
14.	Respondent Contract Signature Deadline	2:00 p.m.	September 30, 2015

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
15.	Anticipated Contract Start Date (anticipated date for contract to be fully executed and vendor to begin work		October 15, 2015

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.

	QUESTION / COMMENT	STATE RESPONSE
1	Regarding items A.30 Performance Standards and Liquidated Damages and E.12. Liquidated Damages; if a vendor takes exception to these items, will their response be deemed unresponsive and/or rejected? If not, please clarify what exceptions / accommodations will the State make?	No. Please reference B.20 in Attachment B of the RFQ.
2	Regarding items A.30 Performance Standards and Liquidated Damages and E.12. Liquidated Damages; Please define all 'contractor actions.'	Contractor Action: Something done or performed by the contractor, typically to achieve an aim.
3	Regarding items A.30 Performance Standards and Liquidated Damages and E.12. Liquidated Damages; Can the vendor propose liquidated damages for the State's failure to fulfill certain obligations as well?	No.
4	Regarding items A.30 Performance Standards and Liquidated Damages and E.12. Liquidated Damages; Can the vendor propose a maximum liquidated damage amount over the duration of the contract?	Yes. Please reference B.20 in Attachment B of the RFQ.
5	Regarding Attachment H, Pro Forma Contract, item A.18., c. Warranty Coverage, we would imagine that for any vendor, if approved specifications do not become the standard for how warranty is to be applied, there is concern as to the determination of warranty scope, timeframes and costs per how this requirement is drafted and potential for endless redefinition of requirements. If a vendor takes exception to, or adds limitations or hourly rates to fulfill these Warranty Coverage requirements, will their response be deemed unresponsive and/or rejected? If not, please clarify what exceptions / accommodations will the State make?	Reference A.78 Warranty in Attachment H of the RFQ. Please reference B.20 in Attachment B of the RFQ. Please be sure to not include any cost information in your technical proposal, as prohibited in RFQ Section 3.4.4
6	Regarding Attachment H, Pro Forma Contract, item A.18., c. Warranty Coverage, we would imagine that for any vendor, if	Refer to the State Response to Question/Comment #5.

	QUESTION / COMMENT	STATE RESPONSE
	approved specifications do not become the standard for how warranty is to be applied, there is concern as to the determination of warranty scope, timeframes and costs per how this requirement is drafted and potential for endless redefinition of requirements. If the vendor will limit warranty the system within a specified timeframe (such as 90 days), will that not be acceptable to the State?	
7	Regarding Attachment H, Pro Forma Contract, item A.18., c. Warranty Coverage, we would imagine that for any vendor, if approved specifications do not become the standard for how warranty is to be applied, there is concern as to the determination of warranty scope, timeframes and costs per how this requirement is drafted and potential for endless redefinition of requirements. The way this requirement is worded, it implies that the State is seeking a custom developed software solution that will be coded to the State's requirements. Is the State not seeking a COTS solution?	The State is amenable to a COTS solution that can be tailored to our specific needs. Refer to the State Response to Question/Comment #5.
8	Considering the length and complexity of this RFQ, as well as that answers to vendor questions being provided Friday, August 7th, and RFQ responses being due Monday, August 17th, only 10 days later, we are concerned that the time available to consume answers to questions, produce, and submit a quality response is not adequate. Additional concerns with available time include the collection of client reference forms in the specified format. Would the State consider extending the Proposal due date? Can the due date be extended by 2 weeks?	The State has extended the response date in Amendment 1 to this RFQ.
9	To help us prepare our cost proposal to the State, do you mind send me an editable version of RFQ #32505-00215 Exhibit E in either Excel or Word format?	Yes. The cost proposal RFQ Attachment D will be provided as a Word document.
10	Under Appendix 3, there is a listing of 69 distinct license, registration and certification types. Can we confirm that this is the total number of business processes that TDA is looking to have automated in the new solution?	Yes, that is confirmed at this date.
11	Reference Appendix 6: pg. 6 - Business Process Re-engineering regarding TDA having documented the current "As Is" business processes. To assist bidders in understanding the nature	Copies will be provided to the successful bidder upon execution of the contract.

	QUESTION / COMMENT	STATE RESPONSE
	and complexity of the current business process workflows, will TDA provide copies of this documentation?	
12	Reference Appendix 6: Pg. 7 - Table 3 - BPR Requirements CR 47 - Where "As Is" documentation does not exist, the Contractor shall…. To assist with quantifying the BPR effort, how many of the business process workflows do not currently have "As Is" documentation?	None
13	Reference Appendix 6: In order to quantify the effort, duration and associated firm fixed pricing associated with the BPR exercise, will TDA accept a set duration for the BPR exercise, and if so what time frame from start to finish is TDA looking to set aside for this?	The proposal should include a recommendation that can be evaluated along with the other components of the proposal. See RFQ Attachment C, Item #C.19.
14	Pg. 7 – Table 3 - CR47 – CR 53. To clarify, is it TDA's intent to have the Contractor review ***all*** "As Is" business processes, document findings, develop recommendations, recommend process improvements (including benefits, ROI, impacts and steps), prioritize recommendations with TDA, develop "To Be" process maps and deliver an implementation plan before commencing configuration efforts?	It is not required that all business processes be reviewed before configuration can begin.
15	As referenced under Appendix 6, pg. 1 – Project Initiation, "*significant access and involvement from TDA staff*" will be required along with timely decision-making to complete the BPR exercise in a timely fashion. With a project start date of Sept. 30, 2015, project initiation activities occurring during the month of Oct., 2015, the BPR exercise requiring likely a minimum of two months of joint TDA/Contractor effort (with anticipated less access to TDA resources in the latter half of Dec.) and assuming all is on schedule, **this would leave a maximum of 6 weeks** for installation, configuration, interfaces, data conversion, system testing, UAT and reports development before moving into production for the first go-live date of Mar. 1, 2016. Attachment C – Pg. 24 under Technical Response and Evaluation Guide, item C.4	The timeline of Stages 1A & 1B are mandatory. Stages 2-5 the State will consider an optional phased proposal. Please reference question 8 of this Amendment.

	QUESTION / COMMENT	STATE RESPONSE
	states; "Describe your company's approach to meet project deliverables and **required milestones** to satisfy **mandatory implementation timeframe** based on the defined scope and requirements RFQ Based on the above, is TDA open to recommendations from the Respondents regarding the project schedule and will, and will proposals be disqualified that don't adhere to the RFQ required milestones and mandatory implementation timeframe?	
16	In Attachment A – Section A – Mandatory Requirement Items, pg. 16, item A.7 states that the Bidder is to *"Provide written confirmation that the Respondent's proposed solution will provide the features and functions or their equivalent included in Appendix 2 – Functions and Technical Requirements, to Attachment H. Pro Forma Contract."* In the Appendix 2, under the Instructions tab it states: "*Respondents may enter comments in the "Comments" column to provide information on that feature such as, it is an out of box solution, it will require customization, or* ***cannot provide the feature or function****.* For clarification, are all of the functional and technical requirements listed in Appendix 2 considered to be mandatory and if so, will a response of "cannot provide the feature of function" disqualify the respondent?	The proposer will not be disqualified, but failure to provide one or more of the functions could affect the final score. See revised RFQ Attachment A, item A.7, and revised RFQ Attachment H, Appendix-2, Instruction tab.
17	Regarding Attachment H – pg. 66, A.30. Performance Standards and Liquidated Damages – is TDA prepared to entertain alternate contractual mechanisms that mitigate risk of system performance rather than the burdensome Liquidated Damages clauses itemized in this Attachment?	Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
18	As a decision to proceed with investing in a response to the RFP will not be made until all answers to questions are received and reviewed, will TDA consider extending the proposal deadline Sept. 4, 2015 - 4 weeks from the date that all answers to questions are provided?	Please reference question 8 of this Amendment.
19	RFQ Appendix 9 - Enterprise information Security Policies, 4.2.1: We request the removal of this requirement, *"4.2.1 OIR Security Management reserves the right to seize any compromised system for forensic analysis"* as it is not applicable	This requirement as started can be waived. The Cloud Service Provider must provide proof that any infected device has been cleaned.

	QUESTION / COMMENT	STATE RESPONSE
	to multi-tenant cloud-based solutions. This requirement applies to on-premise solutions. The Cloud Service Provider offers logs for forensic analysis for a fee. Can the State please adjust the RFQ accordingly for multi-tenant cloud-based solutions?	
20	RFQ Appendix 9 - Enterprise information Security Policies, 4.4.5: We request the removal of this requirement, *"4.4.5 All non-State provided or managed systems storing, processing or transmitting State data should be synchronized to State approved time synchronization services"* as it is not applicable to multi-tenant cloud-based solutions. This requirement applies to on-premise solutions. As part of the service provided by the Cloud Services Provider, clocks of relevant information processing systems are synchronized at least hourly with NTP using Global Positioning System (GPS) as the source. Internal system clocks are used to generate time stamps for audit records. Can the State please adjust the RFQ accordingly?	Cloud Services Provider clocks must synchronize time services to a stratum 0 device.
21	RFQ Appendix 9 - Enterprise information Security Policies, 4.5.1: We request the removal of this requirement, *"4.5.1 Only software that has been licensed and approved as a State standard software product or that has been approved as an exception through the State's architecture standards approval process should be installed on devices covered by the software's license agreement"* The Cloud Services Provider is a single unified service where the underlying mechanisms are transparent to the State. Can the State please adjust the RFQ accordingly for multi-tenant cloud-based solutions?	This requirement can be waived.
22	RFQ Appendix 9 - Enterprise information Security Policies, 5.2.2.1: We request the removal of this requirement, *"5.2.2.1 All State user accounts will follow a State approved standardized naming convention"* as it is not applicable to multi-tenant cloud-based solutions. This requirement applies to on-premise solutions. The Cloud Services Provider only requires an @, so user account names look like email addresses. Is this permissible? Can the State please adjust the RFQ accordingly?	This requirement can be waived.

	QUESTION / COMMENT	STATE RESPONSE
23	RFQ Appendix 9 - Enterprise information Security Policies, 8.2.4: We request the removal of this requirement, *"8.2.4 When exchanging or sharing information classified as Sensitive or Confidential with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party."* as it is not applicable to multi-tenant cloud-based solutions. This requirement applies to on-premise solutions. The Cloud Services Provider has standard confidentiality and non-disclosure terms included as part of the end user licensing agreement that we can share with the State. Are these acceptable? Can the State please adjust the RFQ accordingly?	Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
24	RFQ Appendix 9 - Enterprise information Security Policies, 16.1.2: We request the removal of this requirement, *"16.1.2 All agencies should ensure that their full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who use State of Tennessee resources have read and accept the terms of the relevant State's Acceptable Use Policies. Proof of employee acceptance and acknowledgement will be maintained by the agency"* as it is not applicable to multi-tenant cloud-based solutions. This requirement applies to on-premise solutions. The Cloud Services Provider has existing language in its end-user licensing agreement and cannot have individuals sign/agree to customer specific terms and can share these with the State. Are these acceptable? Can the State please adjust the RFQ accordingly?	This requirement can be waived.

	QUESTION / COMMENT	STATE RESPONSE
25	RFQ Attachment H, Pro Forma Contract, A.38.3, item 3: The Cloud Service Provider uses external service providers to perform application vulnerability assessments. Executive reports for these assessments are available for customers (under NDA) upon request. Cloud Service Provider customers can perform penetration testing of the service after completing a specific Security Assessment Agreement. We request that the State adjust this requirement accordingly to align to what is provided by the Cloud Service Provider. Can the State please adjust the RFQ accordingly?	We cannot agree to this without seeing the Security Assessment Agreement.
26	RFQ Attachment H, Pro Forma Contract, A.48: Cloud Service Provider promptly notifies Customer within 48 hours in the event the Cloud Services Provider becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by the Cloud Services Provider support, email to customer's administrator and Security Contact (if submitted by customer). We request that the State adjust this requirement accordingly to align to what is provided by the Cloud Services Provider. Can the State please adjust the RFQ accordingly?	No, we will not adjust the RFQ. We want the Cloud Service Provider to notify us of an actual or reasonably suspected unauthorized disclosure of Customer Data within 48 hours.
27	RFQ Attachment H, Pro Forma Contract, A.57: This requirement is not applicable to a multi-tenant cloud-based solution. As a multi-tenant cloud-based solution, the Cloud Service Provider provides all the necessary hardware and infrastructure as part of the service. One of the many benefits of multi-tenancy is economies of scale and this gives us great elasticity. We can add hundreds of thousands of users without adding any hardware. This makes such planning unnecessary. We request that the State adjust this requirement accordingly to align to what is provided by the Cloud Services Provider. Can the State please adjust the RFQ accordingly?	This requirement can be waived.
28	RFQ Attachment H, Pro Forma Contract, A.19: The Cloud Service Provider has maintained high levels of availability across	No. Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.

	QUESTION / COMMENT	STATE RESPONSE
	all instances since inception. The Cloud Service Provider uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which the Cloud Service Provider gives customers prior notice, and force majeure events. Support service levels are generally defined by the service provider and based on the level of support purchased by the customer. We request that support service levels be removed or negotiable to a lower level based on the Cloud Service Provider chosen. Can the State please adjust the RFQ accordingly?	
29	RFQ Attachment H, Pro Forma Contract, A.73: Is the State amenable to an RPO and RTO timeframe other than the 1 hour and 4 hours as presently required? During the previous RFQ procurement, the State replied, *"Yes, TDA is amenable to an increase of the RTO up to 48 hours and RPO up to 24 hours"*	Yes, TDA is amenable to an increase of the RTO up to 48 hours and RPO up to 24 hours. This is the current SLA TDA has with the Office of Information Resources Disaster Recovery section. Reference A.73 in Attachment H of the RFQ.
30	RFQ Attachment H, Pro Forma Contract, A.63: This requirement is inapplicable to software delivered as a service subscription through a multi-tenant cloud architecture. The cloud solution being proposed is a Software as a Service (SaaS). System performance monitoring, testing, and capacity planning is part of the service. Customers can do load testing as part of the solution implementation. Can the State please remove/adjust this requirement accordingly for multi-tenant cloud-based solutions?	**Benchmark Tests.** The Contractor shall work with the State to ensure the State has available to it, in a readily useable format, that information which is needed, and the tools which are necessary, in order for the State to conduct and manage effective capacity and performance planning and testing.
31	RFQ Attachment H, Pro Forma Contract, A.62: Cloud Service Provider customers can log cases for support and see all cases logged in their support portal. However, a specific list/log is not provided each month. Can the State please adjust/modify this requirement accordingly to align to multi-tenant cloud-based solutions?	**Maintenance Log.** At minimum, the Contractor shall make available for export from the support portal the following pieces of data related to support: 1. Date and Time of call; 2. Name of Caller; 3. Caller's Organization Name; 4. Caller's telephone number and/or email address; 5. Description of Reported Problem/Complaint; 6. Indication of whether the problem/compliant was resolved at time of call;

	QUESTION / COMMENT	STATE RESPONSE
		7. Description of any follow-up investigation/resolution plans; 8. Assigned Case number and 9. Date, Time and Description of Final Resolution. The export must be provided directly from the portal in either or both .csv and .xls format.
32	RFQ Attachment H, Pro Forma Contract, A.64: This requirement is inapplicable to software delivered as a service subscription through a multi-tenant cloud architecture. The cloud solution being proposed is a Software as a Service (SaaS). System performance monitoring, testing, and capacity planning is part of the service. Can the State please remove/adjust this requirement accordingly for multi-tenant cloud-based solutions?	**Capacity Planning.** The Contractor shall work with the State to ensure the State has available to it, in a readily useable format, that information which is needed, and the tools which are necessary, in order for the State to conduct and manage effective capacity and performance planning and testing.
33	RFQ Attachment H, Pro Forma Contract, E.5: This requirement is inapplicable to software delivered as a service subscription through a mult-itenant cloud architecture. The cloud solution being proposed is a Software as a Service (SaaS) that will be configured to meet the State's specific requirements. Therefore, source code cannot be provided to the State. Can the State please remove/adjust this requirement accordingly for cloud-based solutions?	Please refer to section B.20 of Attachment B of the RFQ.
34	The State has removed all mandatory requirements that outlined FedRAMP in the last RFP. Can the State indicate why FedRAMP requirements were removed in the new RFP release? There are several proven FedRAMP certified solutions on the market.	At the State's request, the contractor shall provide proof of certification, accreditation, or audit on a yearly basis to the State to validate the hosting solution security. (Examples: SOC 2 Type II/ SOC 3, ISO 27001). See revised RFQ Attachment H, item A.53.
35	The State's response to vendor question and comments date is Aug 7th, only 5 workdays away from the proposal due date of Aug 17th, which leaves vendors extremely limited time to make necessary changes to reflect the State's requirement updates, mark the page of each evaluated item and turn in 20 copies as required. For this reason, will the State please consider either publish its response on an earlier date, or postpone the current proposal due date for one week to allow bidding vendors sufficient time to compose comprehensive proposals?	Please reference question 8 of this Amendment.

	QUESTION / COMMENT	STATE RESPONSE
36	We have secured the required bank reference and credit reference letters as required in the State's previous RFQ # 32505-00115. Since these letters are issued in May as we prepare for our response to the canceled RFQ, these letters will be a few days ourside the three (3) months range as required by the State. Given that the requirements have not changed, can the State consider revise the three (3) months limit into four (4) months so we could submit our reference letters without asking our vendors and bank to re-issue those same documents?	Yes.
37	The RFQ Appendix 2, Functional and Technical Requirements shows some requirements with green backgrounds. What is the purpose of these markings?	Please refer to the notice released with the RFQ 32505-00215.
38	Please specify the record types (licenses, permits, certifications) in Appendix 4 Reports and Appendix 5 Forms, that need to be completed in stage 1A and stage 1B.	Those listed for Dairy, Food Safety, Tobacco, Weights & Measures, and Petroleum quality.
39	Can the State confirm that the Contractor is permitted to employ offshore resources for work (such as report development) where state data is not utilized.	Yes, as long as there is not state data transferred offshore for development work.
40	The State has provided information of data that has to be converted into the new system in Amendment 4 #144 of the canceled RFQ# 32505-00115. Please confirm if data conversion demand stays the same, and indicate the stage (1A, 1B, 2, 3, 4, or 5) of delivery.	At this time, Name = Red Barn Vendor = In-house DB Type = SQL Approx. 81,000 of Base Records in 487 Tables Vendor = External Vendor for Food/Dairy/Weights & Measures/Fuel Quality DB Type = SQL Approx. 19,214,149 Rows in 382 tables
41	Is the State willing to negotiate in good faith on terms and conditions of the contract, including performance penalties and damages?	Please reference B.20 in Attachment B of the RFQ. Please also reference RFQ Section 5.5.
42	Given the procurement timeline through final contract execution, there is a very aggressive timeline of approx. 5 months to meet a Phase 1a go live of March 1, 2016. Will the State consider optional proposals	Yes, if the equivalent functionality is available for the programs listed in 1A and 1B. Stages 2-5 the State will consider an optional phased proposal.

	QUESTION / COMMENT	STATE RESPONSE
	for a phased approach?	
43	What is the driver for the March 1, 2016 deadline for Phase 1a?	The contract with the outside vendor for these programs expires on 2/29/16.
44	C.35. Does the State have a document management system to handle scanning, uploading, attaching, document metadata, document lookup/retrieval, document retention, document archiving, version control, etc. as defined in RFQ, that it wishes to interface with the solution, or is the vendor to include a third paty solution for these functions?	The vendor may include a third party.
45	Can the State define which license types from Appendix 3 are included in each Phase? Is the State flexible with the segmentation in order to meet the first go live date?	Reference A.4 in Attachment H of the RFQ. Reference Appendix-2 in Attachment H of the RFQ.
46	Can the RFQ response be removed from the contract?	No. Please refer to D.31 of the pro forma contract.
47	Can the warranty period be reduced to 30 days?	No.
48	The TDA System Milestones are very aggressive, especially when prescribing the methodology that must be followed. Can the milestone dates be modified based on the results of the initial planning and discovery sessions?	Refer to the State Response to Question/Comment #42.
49	There is insufficient time available to perform BPR and meet the specified schedule; can the schedule be adjusted based on the results of the initial planning and discovery sessions?	Refer to the State Response to Question/Comment #42.
50	There is insufficient time to document the "As Is" business processes if they are not already document, and still meet the specified schedule. Can the "As Is" documentation be removed from scope?	"As is" Documents will be provided to the successful bidder upon execution of the contract.
51	Is there a warranty period after the individual phases, or only after the entire project is completed? (after phase 5)	Reference A.78 in Attachment H of the RFQ. The Warranty period begins with the date the Contractor completes the requirements of Implementation Stage 5 as set forth in RFQ Attachment H, Appendix 6, Table 8, System Implementation Phase Requirements certifying full functionality of the System for the last Stage 5.
52	The data cleansing tasks require knowledge of the existing systems, business processes, and ordinances that have impacted the data over the prior years. As such, can the individual departments that	Yes Reference A.75 in Attachment H of the RFQ.

	QUESTION / COMMENT	STATE RESPONSE
	own the data complete the data cleansing tasks?	
53	Can the State designate which reports from Appendix 4 are required for each phase?	Reference A.4 in Attachment H of the RFQ and the revised Appendix 4. .
54	Is the State open to consolidation of reports if filters and variable can be used to result in the information?	Yes
55	Can the State designate the number of staff to be trained per Phase – Administrator and Users?	Reference revised RFQ Attachment H, Appendix 6, Table 10.
56	Can the state provide the size, # of tables, columns, and rows for each database required for conversion?	Refer to the State Response to Question/Comment #40.
57	Will state allow the 'software as a service' model, i.e. instead of the application being hosted by the state, it would be hosted at a 3rd party data-center, with the vendor handling all code maintenance and updates to the software?	Yes
58	Is the ability for TDA staff to create forms within the system a mandatory requirement?	No
59	If TDA produces a form, would it suffice for the system developers to integrate them into the system?	Yes
60	Will developing a list of required reports and specific queries needed fulfill the requirement of ad-hoc reports? If not, is this a negotiable request?	Yes
61	Can more detail be provided on the statewide information to be aggregated?	Refer to the State Response to Question/Comment #40.
62	Is the importation of data into the new system a critical need expected to happen frequently?	Yes see RFQ attachment-H item A.44
63	If the state provides the vendor with the data to import, will this fulfill this requirement?	Reference A.76 of Attachment H of the RFQ. Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
64	If the vendor provides two operating environments which cover the needs of the four operating environments requested, will this suffice?	No Reference A.58 of Attachment H of the RFQ. Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
65	Is offline/remote access required for iOS devices? If the vendor can provide offline/remote access for Windows-based devices, will this suffice?	Yes Windows based devices will suffice
66	Will the state need to work with the outside contractor that developed the systems currently in use? If so, can the name of the contractor(s) be provided?	The State intends to work with current Contractor until contract expires. Digital Health Department (DHD)

	QUESTION / COMMENT	STATE RESPONSE
67	Which legacy systems will content need to be converted from?	Refer to the State Response to Question/Comment #40.
68	Which third-party entities will the vendor need to integrate with?	Link2Gov Corp, an affiliate of Fidelity Information Services, LLC two-way (request/response) API for credit card processing USALIMS Two-Way API(s) for laboratory sample collection and analysis. iNovah Two-Way API for financial transactions. Possible Revenue, SOS, US Postal service two-way APIs for entity and/or postal validation.
69	Is a full, detailed employment history for all vendor staff members required?	No – see RFQ Attachment B item B.13.
70	If not based in Tennessee, is the vendor expected to fulfill the requirement of providing existing programs and procedures designed to encourage and foster commerce with business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises?	Participating with Diversity Business is not a requirement, however it is being evaluated.
71	Can a copy of the Tennessee Business Solutions Methodology be provided?	http://www.tn.gov/finance/article/tbsm which may be updated over time
72	If the vendor can provide a comparable business method that has been proven to work for other projects of this scope, may it be used in place of the TBSM?	The contractor will be required to utilize these templates or templates comparable to the TBSM. See Appendix 6 of RFQ Attachment H.
73	Is it mandatory for vendor staff to perform on-site through the duration of the project? If not mandatory, what is the minimum expectation for on-site availability?	Reference A.8 of RFQ Attachment H. Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
74	May customer references be provided by state employees from states other than Tennessee?	Yes.
75	Is the expected number of users of the system 250?	The expected number of Authorized users is ~250.
76	Are the Performance Standards and Liquidated Damages terms mandatory for a COTS system?	Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
77	Is there a current method in place to ensure that delays specified in the System Performance and Availability requirements are not caused by the State?	Yes
78	Will questions (along with the answers provided by TDA) submitted by other vendors be made available? If so, may we request a copy of these in advance?	All submitted questions and State responses are included in this Q&A amendment
79	Stage 5 (Pesticides) Go Live date has been mentioned as 02-1-17. In Section A.18 -> h. it is mentioned that "...the State to perform all services required by this Contract, including providing a fully implemented Stage 1a of the System suitable for the	Reference A.4 in Attachment H of the RFQ.

	QUESTION / COMMENT	STATE RESPONSE
	needs of by no later than March 1, 2016 and all remaining implementation stages no later than January 1, 2017 ..." Please confirm the Stage 5 Go live date.	
80	Please clarify whether the proposed solution should cater to multiple languages? If yes, kindly specify the languages	No
81	Please let us know if State has any enterprise/organizational guidelines on Integration approach? Ex. Is there any guidelines to integrate the 2 system through a middleware?	No guidelines are available at this time.
82	Is the vendor responsible for performing data cleansing/de-duplication activities? If so, can you elaborate on the assistance you will provide? For example, would Tennessee provide resources to assist in identifying data issues and cleansing data?	Reference A.75 in Attachment H of the RFQ.
83	What format is the source data for conversion in?	The source data is located within a SQL database
84	For the data/documents/collaterals to be migrated in the To-Be system: what is the volume of data to be migrated broken by independent entities/objects/tables?	Refer to the State Response to Question/Comment #40.
85	Would the State consider a comprehensive 100% cloud-based solution designed specifically for the public sector that cannot be hosted in State facilities? How will both “cloud” and “on-premise” solutions be graded and evaluated against the other?	100% cloud based is acceptable. The State will not be hosting. Please reference pro forma Sections A.33 and A.57.
86	Did the State evaluate solutions that could meet its requirements through vendor demonstrations leading up to the RFQ re-issue? If so, what types and names of solutions and vendors were evaluated (vendor-hosted and on-premise)?	No.
87	As per Attachment H, item A. 23, the State indicates that there will be a minimum of 250 users needing access to the proposed system, please confirm if correct. How many will be field/mobile users?	110 to 150 mobile users
88	Does the State have a budget allocated for this project? If so, will the State provide the dollar amount?	The state has tentatively allocated 4 – 6 million dollars for this project.
89	Please confirm that all the functional, technical and interface requirements have been defined in the RFP.	Yes, as of this RFQ release
90	Will the State need off-line inspection capability for remote areas, as part of this project or at a later date?	This capability is needed for this project.
91	Appendix 2:Applications, Permits & Renewal	http://share.tn.gov/sos/rules/0080/0080.htm

	QUESTION / COMMENT	STATE RESPONSE
	#1002 - An error message of "Page Not Found" is received when trying to access the URL. Please provide the URL again.	
92	Appendix 2:Applications, Permits & Renewal #1003 - An error message of "Page was not found" is received when trying to access the URL. Please provide the URL again.	http://tn.gov/agriculture/section/ag-licenses
93	Appendix 2:Applications, Permits & Renewal #1504 - Please point to the section or group of applications that currently create the most challenge for customers in determining what applications are required to complete.	Pesticide Applicators
94	Appendix 2:_Applications, Permits & Renewal #2606 - Please provide an example of a common use case.	Pest Control Companies must have a charter. Each chartered company must have licensed operator who can supervise certified technicians. All of them are related to one entity.
95	Appendix 2:_Bill & Fee Collection #4002 - What is the nature of the interface (xml,REST, SOAP, etc.)?	Currently an encrypted interface system is in place for passing financial information. The protocol for this interface is https. It is RESTful. The State's third party vendor is developing a Token based API for future use. The estimated availability for the Token based API would be sometime in 2016.
96	Appendix 2_Bill & Fee Collection #4205 - If a credit card payment was declined, does that still need to show up as a 'bad payment' since it would not be processed?	No
97	Appendix 2_Bill & Fee Collection #4012 - How are payments processed at the Department of Revenue? What payment gateway, if any, is the Department of Revenue currently using?	See revised #4012 in Appendix 2 of RFQ Attachment H.
98	Appendix 2_Bill & Fee Collection #4806 - The State has highlighted this requirement as being changed, and yet upon comparison to the original RFQ (#32505-00115) the wording is a direct copy. How does this requirement differ to the original RFQ?	Requirement did not change.
99	Appendix 2_Inspection Management #5106 - Does the proposed solution need to provide offline and online capabilities for collecting field samples on portable devices? Please state the type of portable devices used.	Yes it needs to function online and offline. The State is open to considering portable devices recommended by the contractor.

	QUESTION / COMMENT	STATE RESPONSE
100	Appendix 2_System Common #10006 - Would an external link displayed on the application page suffice for the applicant to look up regulations?	Yes, if it were linked to a specific rule section and not a general site like the Secretary of State's office.
101	Appendix 2_System Common #10014 - What 3rd partyprocessor is to be integrated with?	Link2Gov Corp, an affiliate of Fidelity Information Services, LLC
102	Appendix 2_System Common #11402 - Does the State haveexisting reader/scanner equipment or do they want this proposal to recommend hardware? If we are to recommend hardware, how many scanning points (in and out) are anticipated?	The state has scanning equipment. n/a
103	Appendix 2_System Common #11802 - Does the State have existing 1D reader/scanner equipment or do they want this proposal to recommend hardware? If we are to recommend hardware, how many scanning points (in and out) are anticipated?	The state has scanning equipment.
104	Appendix 2_Mobile Access #8008 - The State has highlighted this requirement as being changed, and yet upon comparison to the original RFQ (#32505-00115) the wording is a direct copy. How does this requirement differ to the original RFQ?	Requirement was not changed.
105	Regarding "Inspection Information" requirement #8006, can the State elaborate on the need for mobile inspection/field investigation capabilities? (a) What type of device(s) does the state have, or is planning to acquire for this project?	The purpose of this project is to allow field inspections to be performed electronically with access to previous inspection reports without the need for paper files for review. The inspector must be able to record all required inspection information and submit the report. The state currently has iPads and Microsoft devices.
106	Regarding "Inspection Information" requirement #8006, can the State elaborate on the need for mobile inspection/field investigation capabilities? Does the State have a preference for mobile device Operating System (OS)? IOS or Android?	The purpose of this project is to allow field inspections to be performed electronically with access to previous inspection reports without the need for paper files for review. The inspector must be able to record all required inspection information and submit the report. The state currently has IPad and Microsoft devices. Android is not an option.
107	Regarding "Inspection Information" requirement #8006, can the State elaborate on the need for mobile inspection/field investigation capabilities? Would the agency need to use its own devices and mobile service, or could it pursue an all-inclusive solution integrated with its backoffice system?	Refer to the State Response to Question/Comment #106. The State would consider an all-inclusive system.
108	Regarding "Inspection Information" requirement #8006, can the State elaborate	Refer to the State Response to Question/Comment #106.

	QUESTION / COMMENT	STATE RESPONSE
	on the need for mobile inspection/field investigation capabilities? In order that we may determine the number of forms that would be integrated into the new mobile system, how many different forms are currently in use in the field?	Approximately 100
109	Regarding "Inspection Information" requirement #8006, can the State elaborate on the need for mobile inspection/field investigation capabilities? How should pricing for these items be proposed?	Refer to the State Response to Question/Comment #106. Reference Attachment E of the RFQ.
110	Requirement #10811, "Workflow Automation", requires 'viewing of the existing Workflows in both text and diagram form." Please elaborate as to the State's expectation for how / what they envision to fulfill this requirement?	For the purpose of review and revision workflows should be viewable.
111	Regarding Appendix 2, Functional and Technical Requirements, on the tab System Common, #12301 The system should comply with the respective State Directory Service Specifications. Please provide the State Directory Service Specifications.	Delete item #12301 in Appendix 2 of RFQ Attachment H.
112	Please elaborate upon the database architecture and how the State envisions a COTS vendor's solution is to be made to conform to the infrastructure referenced in "Database" requirement #12907.	Refer to the State of Tennessee Enterprise Technology Architecture Standard Products provided to you by Contract and Procurement Office.
113	Regarding requirement #13104, (1) Please specify the entire testing scenario for measuring usability guidelines, including all steps taken, and from what start-point to end-point the timing would be measured.	Delete item #13104 in Appendix 2 of RFQ Attachment H.
114	Regarding requirement #13104, Please confirm these would be measured at the server without interference of network or internet traffic.	Delete item #13104 in Appendix 2 of RFQ Attachment H.
115	Regarding requirement #13104, Please specify any bandwidth or network requirements to be factored into these calculations.	Delete item #13104 in Appendix 2 of RFQ Attachment H.
116	Regarding requirement #13104 Please describe the details of the most complex report/search which must be run in under 10 seconds.	Delete item #13104 in Appendix 2 of RFQ Attachment H.
117	Regarding item A.5, (1) please define 'accredited credit bureaus' and what is 'a positive credit rating'.	Please reference the 3 main credit bureaus: Equifax, Experian, and TransUnion.
118	Regarding item A.5, We are a privately owned company and no data is collected from credit bureaus, is this a problem?	Privately owned companies will still have credit reports.
119	Regarding item A.5 If there is not enough information collected for a report, will that vendor's response be disqualified?	The State has the discretion to disqualify.

	QUESTION / COMMENT	STATE RESPONSE
120	In Appendix 6, Summary of Services, what kind of testing tools are meant by " The Contractor shall license testing tools for use by the State. "?	Any testing tools utilized by the Contractor which require licenses for State users to meet the requirement of the Contract.
121	Regarding A.8.a.2., "If the State Project Manager does not agree to the replacement of Key Project Staff and does not wish to terminate the Contract, the Key Project Staff member must remain on the Project and must continue to work with the same degree of professionalism he or she provided prior to the Contractor's request for removal. If the Key Project Staff fails to do so, or if the Contractor removes the Key Project Staff without the State Project Manager's consent, the State has the right to terminate as indicated in D.6 or assess liquidated damages as described in *Pro Forma* Contract Section A.30. - Performance Standards and Liquidated Damages." Does that State agree that this statement does not apply to Key Project Staff members who choose to leave the contractor's employment?	Yes
122	Regarding A.8.c. The Contractor's team members who have been defined as full-time (100% of working time) within the Master Project Schedule (Contractors' Team), shall perform their duties on-site in Nashville, Tennessee, , unless otherwise agreed to by the State in writing. Non full time Contractor staff is not required to be based in Nashville, TN, but shall be available to be on site during their active periods of project engagement, as reasonably requested by the State Project Manager. All team members working onsite shall be identified to the State, along with any Contractor issued equipment intended to be used on site. Does the State require a full-time team member from the Contractor?	No Reference B.20 in Attachment B of the RFQ, any contract changes should be included as a redlined contract version.
123	If a vendor does not comply to the TBSM model for project management, however does utilize a comparable Project Management Methodology proven in multiple similar, successful implementations, will that vendor be disqualified?	No
124	Regarding item A.38. Assessment of the System, please define what constitutes a "significant event", and how the State will perform reassessments.	Any new or major code releases.
125	We have a Named User licensing structure. We define Named Users as "staff with access to the back-office Software regardless of whether such access is concurrent or consecutive." Based on this	Approximately 140

	QUESTION / COMMENT	STATE RESPONSE
	definition, how many Named Users does the agency anticipate having on its new system?	
126	Your RFP mentions a need for certain third-party data-exchange interfaces. Please provide an inventory of these required system interfaces and the purpose of each. Also, please note if each interface will be one-way or two-way.	Refer to the State Response to Question/Comment #68.
127	Can the State list all the license types the agency supports, and specify which license type(s) will require which types of online functionality (e.g. online applications, renewals, verifications, disciplinary processes, etc.)?	All licenses types are listed in Appendix 3. All of them should have very similar functionality.
128	Please provide the names of all system outputs required, including reports, queries, and correspondences. Also provide the audience and the location from which each will be run (back-office, public website, specific login-secured area of public website, etc.). If such details are not available at this time, please provide at least the total numbers of each type of output required.	Report audiences will be management and public information. The total number of reports will depend upon the contractor's ability to build consistent reporting templates that allow multiple report requirements by selecting unique output criteria. Refer to the State Response to Question/Comment #54.
129	Regarding section A.23. As a COTS software provider, we have a standard license agreement and additional contract terms which need to be incorporated into the procurement process. Where in our response should these appear?	Please reference B.20 in Attachment B of the RFQ.
130	We offer multiple support plan options in addition to the primary support plan we will be proposing. How would you like us to incorporate the additional options and corresponding contract language into our proposal, to provide the agency with the right and option to choose from our full range of support options in the future?	Your proposal must be all inclusive of what the State is requiring. No additional costs may be included.
131	Regarding state registration, we have found it is typically acceptable for the vendor to plan to register only if awarded the contract. Is registration required in advance of the RFP evaluation process, or is it only required in order to finalize a contract with the selected vendor per General Information and Requirements item 4.6?	Registration is required prior to contract signing; it is not a requirement to propose.
132	Please identify instances where any agency employee has discussed, viewed or have been demonstrated potential software applications similar to the one being solicited in this RFQ in the last 24 months. Please name the vendor(s), dates of contact and describe the nature of the contacts, including whether pricing was discussed.	Numerous employees have viewed demonstrations of software applications similar to this solicitation in various venues, including national and regional meetings and conferences. Some vendors have provided demonstrations and written material to staff at their offices. Specific vendors and locations are too numerous to list in this setting.

	QUESTION / COMMENT	STATE RESPONSE
133	We understand/assume the technical support services required post-go-live are as noted in the grid below (X = "Yes"). Please confirm this understanding, or further clarify the support required in each of these and any other categories, so vendors can provide pricing for equivalent support plans: (see table below)	Reference RFQ Attachment H, Appendix 6, Table 11 and 12. Reference Attachment E of the RFQ.

Software Support Services Post-Go-Live	Required to be included in support plan?	To be billed per hour/unit?	Other? (describe)
a. Help Desk Support			
i. 24 x 7 Emergency Support	X		
ii. End-User Support	X		
iii. Configuration Troubleshooting	X		
iv. Developer-to-Developer Support	X		
v. Hardware, Network, and Security Tips		X	
vi. Architecture and Best Practice Guidance		X	
vii. Online Remote Desktop Support		X	
viii. Dedicated Account Management	X		
ix. Local User Group Support		X	
b. Training and Documentation			
i. Web Courses	X		
ii. Agency-Specific Process Training	X		
iii. Software Training	X		
iv. Core Software Documentation	X		
v. User Conference		X	
c. Software Patches and Releases			
i. New Software Versions (major releases)	X		

ii. Installation of New Software Versions		X	
iii. Core Software Patches	X		
iv. Installation of Core Software Patches		X	
d. Customization, Enhancement, and Corrections			
i. Design, Configuration, Testing, Support		X	
ii. Customization Projects		X	
iii. Customization Tasks		X	
iv. Defect Correction	X		
v. Installation of Customization Corrections	X		
e. Hosting Service			
i. Weekly Backup	X		
ii. Daily Backup	X		
iii. Hosting of Company's Proprietary Software	X		
iv. IP Address Owned and Provided by Company	X		
v. Maintenance of Hosting Environment	X		
vi. Data Security	X		
f. Mobile Service			
i. Mobile Devices Provided by Company		X	
ii. Wireless Data Services		X	
iii. Configuration of Forms for Mobile Use		X	
iv. Mobile Inspection Dispatch System		X	

3. **Delete RFQ # 32505-00215, in its entirety, and replace it with RFQ #32505-00215 Release # 2, attached to this amendment.** Revisions of the original RFQ document are emphasized within the new release. Any sentence or paragraph containing revised or new text is highlighted.

4. **Delete RFQ # 32505-00215 Appendix 2 in its entirety, and replace it with RFQ #32505-00215 Appendix 2 Version 2, attached to this amendment.** Revisions of the original RFQ document are

emphasized within the new release. Any sentence or paragraph containing revised or new text is highlighted.

5. **Delete RFQ # 32505-00215 Appendix 4 in its entirety, and replace it with RFQ #32505-00215 Appendix 4 Version 2, attached to this amendment.** Revisions of the original RFQ document are emphasized within the new release. Any sentence or paragraph containing revised or new text is highlighted.

6. **Delete RFQ # 32505-00215 Appendix 6 in its entirety, and replace it with RFQ #32505-00215 Appendix 6 Version 2, attached to this amendment.** Revisions of the original RFQ document are emphasized within the new release. Any sentence or paragraph containing revised or new text is highlighted.

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.

STATE OF TENNESSEE
CENTRAL PROCUREMENT OFFICE

REQUEST FOR QUALIFICATIONS
FOR
TDA LICENSE, INSPECTION, CERTIFICATION SOFTWARE, SERVICES, AND HOSTING

RFQ # 32505-00215

Release #2

TABLE OF CONTENTS

SECTIONS:

1. **Introduction**
2. **RFQ Schedule of Events**
3. **Response Requirements**
4. **General Information & Requirements**
5. **Procurement Process & Contract Award**

ATTACHMENTS:

A. **Technical Response & Evaluation Guide – Mandatory Requirement Items**
B. **Technical Response & Evaluation Guide – General Qualifications & Experience Items**
C. **Technical Response & Evaluation Guide – Technical Qualifications, Experience & Approach Items**
D. **Technical Response & Evaluation Guide- Oral Presentation**
E. **Cost Proposal & Evaluation Guide**
F. **Statement of Certifications & Assurances**
G. **Reference Questionnaire**
H. ***Pro Forma* Contract**
   Appendix 1 – Glossary
   Appendix 2 – Functional and Technical Requirements
   Appendix 3 – Statistics
   Appendix 4 – Reports
   Appendix 5 – Forms
   Appendix 6 – Contractor Requirements
   Appendix 7 – State's Acceptable Use Policy and Acceptance Use Agreement
   Appendix 8 – Non-disclosure Agreement (NDA)
   Appendix 9 – Public Enterprise Information Security Policies
   Appendix 10 – Deliverable Specification Sheet

1. INTRODUCTION

The State of Tennessee, Central Procurement Office, hereinafter referred to as "the State," has issued this Request for Qualifications ("RFQ") to define mandatory goods or services requirements; solicit responses; detail response requirements; and outline the State's process for evaluating responses and selecting a Respondent for contract award to provide the needed goods or services.

Through this RFQ or any subsequent solicitation, the State seeks to buy the requested goods or services at the most favorable, competitive prices and to give ALL qualified businesses, including those owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises, the opportunity to do business with the State as contractors or subcontractors

1.1. Statement of Procurement Purpose

Tennessee Department of Agriculture (TDA), Division of Consumer and Industry Services (CIS) seeks to obtain an enterprise automated solution for regulatory activities in each program area, such as: licensing, inspection, certification, invoicing, revenue collection which will:

- Improve customer service to individuals and businesses in TDA,
- Provide savings through administering TDA Program Area standardization, and avoiding the cost of maintaining multiple independent systems,
- Streamline the administrative process of issuing and regulating TDA licenses, permits, inspections, and certifications.
- Provide a seamless transition from the current system(s) to the new system.
- Provide for unlimited future growth in the number of establishments in each program area.

This contract is seeking a proven Licensing, Inspection, and Certification/Education software solution, with accompanying integration, support/maintenance, and hosting services. TDA seeks an enterprise solution to automate and improve Licensing, Inspection, and Certification/Education. Please refer *to Pro Forma* Contract Appendix 2 - Functional and Technical Requirements for a narrative description of the functional requirements. The selected contractor shall provide the necessary software development tools, personnel, and project management expertise required to fulfill contractual requirements on time within the agreed project schedule. The selected Contractor will provide a solution that supports mobile devices, the mobile devices will be provided by the State.

The State is seeking a proven software solution, that is highly configurable (i.e. can be adapted to meet changing business needs with minimal custom changes to the underlying software programming code) so that TDA staff can create forms, specific workflows and business processes.

The State seeks to provide Inspectors with mobile devices to conduct both online and offline capabilities for conducting Inspections, public online access to apply for license and permit application, renewals, maintenance change needs, status, training, enforcement of rules and other critical needs via a customer web portal and employee portal with an emphasis on efficiency for enforcement services.

The State shall procure these services for the duration of the *Pro Forma* Contract and other services required to complete activities and deliverables as specified in the *Pro Forma* Contract for the project.

Background

The CIS Division is dedicated to the two main objectives of agricultural production quality and consumer protection. Responsibilities of the division include sampling the quality of feeds, seeds, and fertilizers; protecting animal and plant health; registering pesticides; ensuring food safety; and inspecting processing establishments. A laboratory supports regulatory efforts.

The TDA CIS monitors agricultural raw materials, products, and services to assure quality, consumer protection, public safety, a fair market place, and a safe and wholesome food supply. Statutes direct responsibility for the registration, licensing, sampling, inspection of items pertaining to human and animal health safety, consumer protection, truth in labeling, and free movement of plants and animals.

The vision is for a scalable enterprise solution capable of serving all TDA program areas. Currently these program areas are in several independent systems. Some of these independent systems were developed by TDA staff, and are currently maintained in-house. While other program areas, were developed and are currently supported with an outside Contractor. A few program areas and functions may still be handled manually.

The State seeks to improve its current situation through better use of technology, improved and efficient processes and workflow, improved enterprise standard policies and procedures, management and controls, and improved utilization of resources.

The State understands that implementation of an Enterprise system will necessitate organizational change management planning to support the overall implementation.

1.1.1. **Factual Data**

All statistical and fiscal information contained in this RFQ and its exhibits, including amendments and modifications thereto, are provided “as is”, without warranty as to the accuracy or adequacy of the data or information so provided, and reflect the department’s best understanding based on information or belief available to the department at the time of RFQ preparation. No inaccuracies in such data or information shall be a basis for delay in performance or a basis for legal recovery of damages, actual, consequential or punitive.

1.2. Notice of Intent to Respond

Before the Notice of Intent to Respond Deadline detailed in RFQ § 2, Schedule of Events, potential Respondents should submit to the Solicitation Coordinator a Notice of Intent to Respond in the form of a simple e-mail or other written communication. Such notice should include the following information: the business or individual’s name (as appropriate), a contact person’s name and title, the contact person’s mailing address, telephone number, facsimile, number, and e-mail address. Filing a Notice of Intent to Respond is not a prerequisite for submitting a response; however, it is necessary to ensure receipt of notices and communications relating to this RFQ.

Attached to this RFQ is Appendix 8, *Non-disclosure Agreement (NDA).* Potential bidders must send in their “Intent to bid” and the signed NDA. Once the signed forms are received by the State, the State will send a copy of *Tennessee Information Resources Architecture* as referenced in RFQ Attachment H - *Pro Forma* - Section A.20. Prospective respondents must propose any exceptions to standards at the Q&A phase of the solicitation.

1.4. Definitions and Abbreviations

See RFQ Attachment H, Pro Forma Contract, Appendix 1 – Glossary.

2. RFQ SCHEDULE OF EVENTS

The following schedule represents the State's best estimates for this RFQ; however, the State reserves the right, at its sole discretion, to adjust the schedule at any time, or cancel and reissue a similar solicitation. Nothing in this RFQ is intended by the State to create any property rights or expectations of a property right in any Respondent.

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
1.	RFQ Issued		July 17, 2015
2.	Disability Accommodation Request Deadline	2:00 p.m.	July 22, 2015
3.	Notice of Intent to Respond Deadline	2:00 p.m.	July 24, 2015
4.	Written "Questions & Comments" Deadline	2:00 p.m.	July 31, 2015
5.	State response to written "Questions & Comments"		August 11, 2015
6.	RFQ Response Deadline	9:00 a.m.	August 25, 2015
7.	State Notice of Qualified Respondents Released		September 1, 2015
8.	State Schedules respondent Oral Presentations (Only for Qualified Respondents)		September 2, 2015
9.	Respondent Oral Presentations	8:00 a.m. – 4:30 p.m.	September 10-14, 2015
10.	RFQ Cost Negotiations		September 15-16, 2015
11.	State Evaluation Notice Released		September 17, 2015
12.	Solicitation Files Opened for Public Inspection		September 17, 2015
13.	End of Open File Period		September 24, 2015
14.	Respondent Contract Signature Deadline	2:00 p.m.	September 30, 2015
15.	Anticipated Contract Start Date (anticipated date for contract to be fully executed and vendor to begin work		October 15, 2015

3. RESPONSE REQUIREMENTS

3.1 Response Contents: A response to this RFQ should address the following:

3.1.1. Mandatory Requirements: This section details the mandatory technical, functional, and experience requirements that must be demonstrated in the response to this RFQ in order to be passed on to Phase II of the Technical Response evaluation. A Respondent must duplicate and use RFQ Attachment A as a guide to organize responses for the Mandatory Requirements of the RFQ response. The Respondent should reference the page location of the information within the response in the indicated column of the table. This section is included in the State's evaluation as to whether or not a Respondent meets mandatory qualifications (Phase I).

3.1.2. General Qualifications & Experience: This section is included in the State's evaluation of Phase II of the Technical Response Evaluation and details general information and qualifications that must be demonstrated in the response to this RFQ. A Respondent must duplicate and use RFQ Attachment B as a guide to organize responses for this portion of the RFQ response. The Respondent should reference the page location in the information within the response in the indicated column of the table.

3.1.3. Technical Qualifications, Experience & Approach: This section is also included in the State's evaluation of Phase II of the Technical Response Evaluation and details technical qualifications, experience, and approach items that must be demonstrated in the response to this RFQ. A Respondent must duplicate and use RFQ Attachment C as a guide to organize responses for this portion of the RFQ response. The Respondent should reference the page location in the information within the response in the indicated column of the table.

3.1.4. Cost Proposal:

3.1.4.1. If included as part of this solicitation, then the Cost Proposal must be recorded on an exact duplicate of RFQ Attachment E, Cost Proposal & Evaluation Guide. Any response that does not follow the instructions included in RFQ Attachment E may be deemed nonresponsive.

3.1.4.2. A Respondent must only record the proposed cost exactly as required by the RFQ Attachment E, Cost Proposal & Evaluation Guide and must NOT record any other rates, amounts, or information.

3.1.4.3. The proposed cost shall incorporate ALL costs for services under the contract for the total contract period.

3.1.4.4. A Respondent must sign and date the Cost Proposal.

3.1.4.5. A Respondent must submit the Cost Proposal to the State in a sealed package separate from the Technical Response.

3.2. Response Delivery Location

A Respondent must ensure that the State receives a Response to this RFQ no later than the Response Deadline time and dates detailed in the RFQ § 2, Schedule of Events. All responses must be delivered to:

Elizabeth Stafford
Sourcing Analyst
Central Procurement Office
Department of General Services
William R. Snodgrass TN Tower – 3rd Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615 532-0764
E-mail: Elizabeth.Stafford@tn.gov

3.3. Response Format

3.3.1. A Respondent must ensure that the original response meets all form and content requirements detailed within this RFQ.

3.3.2. A Respondent must submit original response documents and copies as specified below.

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

"RFQ #32505-00215 TECHNICAL RESPONSE ORIGINAL"

and twenty (20) copies of the Technical Response each in the form of one (1) digital document in "PDF" format properly recorded on its own otherwise blank, standard CD-R recordable disc or USB flash drive labeled:

"RFQ #32505-00215 TECHNICAL RESPONSE COPY"

The digital copies should not include copies of sealed customer references or cost information in the general and technical evaluation phase. However, any other discrepancy between the paper response document and digital copies may result in the State rejecting the response as nonresponsive.

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

"RFQ #32505-00215 COST PROPOSAL ORIGINAL"

and one (1) copy in the form of a digital document in "XLS" format properly recorded on a separate, blank, standard CD-R recordable disc or USB flash-drive labeled:

"RFQ #32505-00215 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.

3.4. Response Prohibitions: A response to this RFQ shall not:

3.4.1. Restrict the rights of the State or otherwise qualify the response to this RFQ;

3.4.2. Include, for consideration in this procurement process or subsequent contract negotiations, incorrect information that the Respondent knew or should have known was materially incorrect;

3.4.3. Include more than one response, per Respondent, to this RFQ;

3.4.4. Include any information concerning costs (in specific dollars or numbers) associated with the Technical Response;

3.4.5. Include the respondent's own contract terms and conditions (unless specifically requested by the RFQ);

3.4.6. Include the respondent as a prime contractor while also permitting one or more other respondents to offer the respondent as a subcontractor in their own responses; or

3.4.7. Provide an oral presentation to exceed 4 hours in length including time for questions. A topic outline will be provided with the oral presentation invitation.

3.5. Response Errors & Revisions

A Respondent is responsible for any and all errors or omissions in its response to this RFQ. A Respondent will not be allowed to alter or revise its response after the Response Deadline time and dates as detailed in RFQ § 2, Schedule of Events, unless such is formally requested in writing by the State (e.g., through a request for clarification, etc.).

3.6. Response Withdrawal

A Respondent may withdraw a response at any time before the Response Deadline time and date as detailed in RFQ § 2, Schedule of Events, by submitting a written signed request by an authorized representative of the Respondent. After withdrawing a response, a Respondent may submit another Response at any time before the Response Deadline time and date as detailed in RFQ § 2, Schedule of Events.

3.7 Response Preparation Costs

The State will not pay any costs associated with the preparation, submittal, or presentation of any response. Each Respondent is solely responsible for the costs it incurs in responding to this RFQ.

4. GENERAL INFORMATION & REQUIREMENTS

4.1 Communications

4.1.1 Respondents shall reference RFQ # 32505-00215 in all communications relating to this solicitation, and direct any such communications to the following person designated as the Solicitation Coordinator:

Elizabeth Stafford
Sourcing Analyst
Central Procurement Office
Department of General Services
William R. Snodgrass TN Tower – 3rd Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615 532-0764
E-mail: Elizabeth.Stafford@tn.gov

The State will convey all official responses and communications related to this RFQ to the potential respondents from whom the State has received a Notice of Intent to Respond (refer to RFQ Section 1.2.).

4.1.2 Potential respondents with a handicap or disability may receive accommodation relating to the communication of this RFQ and participating in the RFQ process. Potential respondents may contact the RFQ Coordinator to request such reasonable accommodation no later than the Disability Accommodation Request Deadline detailed in RFQ § 2, Schedule of Events.

4.1.3 **Unauthorized contact about this RFQ with other employees or officials of the State of Tennessee may result in disqualification from contract award consideration.**

4.1.4 Notwithstanding the foregoing, potential Respondents may also contact the following as appropriate:

4.1.4.1. Staff of the Governor's Office of Diversity Business Enterprise may be contacted for assistance with respect to available minority-owned, woman-owned, Tennessee service-disabled veteran-owned, and small business enterprises as well as general public information relating to this request; or

4.1.4.2. The following individual designated by the State to coordinate compliance with the nondiscrimination requirements of the State of Tennessee, Title VI of the Civil Rights Act of 1964, the Americans with Disabilities Act of 1990, and associated federal regulations:

Helen Crowley
Central Procurement Office
Department of General Services
William R. Snodgrass TN Tower – 3rd Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615 741-3836
E-mail: Helen.Crowley@tn.gov

4.2. **Nondiscrimination**

No person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of a contract pursuant to this solicitation or in the employment practices of the Vendor on the grounds of handicap or disability, age, race, color, religion (subject to *Tennessee Code Annotated,* Sections 4-21-401 and 405), sex, national origin, or any other classification protected by federal, Tennessee state constitutional, or statutory law. The Vendor pursuant to this solicitation shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

4.3. **Conflict of Interest**

4.3.1. The State may not consider a proposal from an individual who is, or within the past six (6) months has been, a State employee. For these purposes,

4.3.1.1. An individual shall be deemed a State employee until such time as all compensation for salary, termination pay, and annual leave has been paid;

4.3.1.2. A contract with or a proposal from a company, corporation, or any other contracting entity in which a controlling interest is held by any State employee shall be considered to be a contract with or proposal from the employee; and

4.3.1.3. A contract with or a proposal from a company, corporation, or any other contracting entity that employs an individual who is, or within the past six months has been, a State employee shall not be considered a contract with or a proposal from the employee and shall not constitute a prohibited conflict of interest.

4.3.2. This RFQ is also subject to *Tennessee Code Annotated*, Section 12-4-101.

4.4. **Respondent Required Review & Waiver of Objections**

4.4.1. Each potential respondent must carefully review this RFQ, including but not limited to, attachments, the RFQ Attachment H, *Pro Forma* Contract, and any amendments for questions, comments, defects, objections, or any other matter requiring clarification or correction (collectively called “questions and comments”).

4.4.2. Any potential respondent having questions and comments concerning this RFQ must provide such in writing to the State no later than the written “Questions & Comments Deadline” detailed in RFQ § 2, Schedule of Events.

4.4.3. Protests based on any objection shall be considered waived and invalid if the objection has not been brought to the attention of the State, in writing, by the written “Questions & Comments Deadline.”

4.5. **Disclosure of Response Contents**

4.5.1. All materials submitted to the State in response to this solicitation become property of the State of Tennessee. Selection for award does not affect this right. By submitting a response, a Respondent acknowledges and accepts that the full contents and associated documents submitted in response to this request will become open to public inspection. Refer to RFQ § 2, Schedule of Events.

4.5.2. The RFQ responses will be available for public inspection only after the completion of evaluation of the RFQ or any resulting solicitation which this RFQ becomes a part of, whichever is later.

4.6. **Notice of Professional Licensure, Insurance, and Department of Revenue Registration Requirements**

4.6.1. All persons, agencies, firms or other entities that provide legal or financial opinions, which a Respondent provides for consideration and evaluation by the State as part of a response to this RFQ, shall be properly licensed to render such opinions.

4.6.2. Before the Contract resulting from this RFQ is signed, the apparent successful Respondent (and Respondent employees and subcontractors, as applicable) must hold all necessary, appropriate business and professional licenses to provide service as required. The State may require any Respondent to submit evidence of proper licensure.

4.6.3. Before the Contract resulting from this RFQ is signed, the apparent successful Respondent must provide a valid, Certificate of Insurance indicating current insurance coverage meeting minimum requirements as may be specified by the RFQ.

4.6.4. Before the Contract resulting from this RFQ is signed, the apparent successful Respondent must be registered with the Department of Revenue for the collection of Tennessee sales and use tax. The State shall not approve a contract unless the Respondent provides proof of such registration. The foregoing is a mandatory requirement of an award of a contract pursuant to this solicitation.

4.7. **RFQ Amendments & Cancellation**

4.7.1. The State reserves the right to amend this RFQ at any time, provided that it is amended in writing. However, prior to any such amendment, the State will consider whether it would negatively impact the ability of potential respondents to meet the deadlines and revise the RFQ Schedule of Events if deemed appropriate. If a RFQ amendment is issued, the State will convey it to potential respondents who submitted a Notice of Intent to Respond (refer to RFQ § 1.2). A respondent must respond, as required, to the final RFQ (including its attachments) as may be amended.

4.7.2. The State reserves the right, at its sole discretion, to cancel or to cancel and reissue this RFQ in accordance with applicable laws and regulations.

4.8. **State Right of Rejection**

4.8.1. Subject to applicable laws and regulations, the State reserves the right to reject, at its sole discretion, any and all proposals.

4.8.2. The State may deem as nonresponsive and reject any proposal that does not comply with all terms, conditions, and performance requirements of this RFQ. Notwithstanding the foregoing, the State reserves the right to seek clarifications or to waive, at its sole discretion, a response's minor variances from full compliance with this RFQ. If the State waives variances in a response, such waiver shall not modify the RFQ requirements or excuse the Respondent from full compliance with such, and the State may hold any resulting vendor to strict compliance with this RFQ.

4.8.3. The State will review the response evaluation record and any other available information pertinent to whether or not each respondent is responsive and responsible. If the evaluation team identifies any respondent that appears <u>not</u> to meet the responsive and responsible thresholds such that the team would not recommend the respondent for potential contract award, this determination will be fully documented for the record. ("Responsive" is defined as submitting a response that conforms in all material respects to the RFQ. "Responsible" is defined as having the capacity in all respects to perform

fully the contract requirements, and the integrity and reliability which will assure good faith performance.)

4.9. **Assignment & Subcontracting**

4.9.1. The vendor may not subcontract, transfer, or assign any portion of the Contract awarded as a result of this RFQ without prior approval of the State. The State reserves the right to refuse approval, at its sole discretion, of any subcontract, transfer, or assignment.

4.9.2. If a Respondent intends to use subcontractors, the response to this RFQ must specifically identify the scope and portions of the work each subcontractor will perform (refer to RFQ Attachment B, Item B.14.).

4.9.3. Subcontractors identified within a response to this RFQ will be deemed as approved by the State unless the State expressly disapproves one or more of the proposed subcontractors prior to signing the Contract.

4.9.4. The Contractor resulting from this RFQ may only substitute another subcontractor for a proposed subcontractor at the discretion of the State and with the State's prior, written approval.

4.9.5. Notwithstanding any State approval relating to subcontracts, the Contractor resulting from this RFQ will be the prime contractor and will be responsible for all work under the Contract.

4.10. **Next Ranked Respondent**

The State reserves the right to initiate negotiations with the next ranked respondent should the State cease doing business with any respondent selected via this RFQ process.

5. PROCUREMENT PROCESS & CONTRACT AWARD

5.1. The complete vendor selection will be three-part process: (1) Qualification of Technical Responses; (2) Oral Presentation; and (3) Cost Proposals/Negotiations. Any contract award is subject to successful contract negotiation.

5.2. Qualification of Technical Responses: Technical Responses will be short-listed for further evaluation, analysis or negotiation if they are apparently responsive, responsible, and within the competitive range. A Technical Response will be deemed within the competitive range based on the following criterion:

Ranking: To be qualified for the competitive range, the Technical Response must be ranked in the top 4 after the Technical Response score is totaled and put in ordinal ranking (1 - the best evaluated ranking).

Phase I: The State will evaluate the Mandatory Requirements set forth in RFQ Attachment A on a pass/fail basis

Phase II: Following the Phase I evaluation, the State will apply a standard equitable evaluation model, which will represent a qualitative assessment of each response. Each response will be scored by Evaluation Team members according to the Technical Response & Evaluation Guides (See RFQ Attachments B & C.

The Solicitation Coordinator will total the average score from the Evaluation Team for each responsive and responsible Respondent's Technical Response Points for RFQ Attachments B & C. This will determine which of the Respondents are considered Qualified and within the competitive range.

Phase III: The State may invite those within the competitive range after Phase II evaluation to give oral presentations to the State. The qualitative assessment of each Respondent will include the information derived from the oral presentations.

5.3. Oral Presentation: The Solicitation Coordinator will invite each Respondent, who passed Phase II, to make an oral presentation.

5.3.1 The Solicitation Coordinator will schedule Respondent presentations during the period indicated by the RFQ Section 2, Schedule of Events. The Solicitation Coordinator will make every effort to accommodate each Respondent's schedules. When the Respondent presentation schedule has been determined, the Solicitation Coordinator will contact Respondents with the relevant information as indicated by RFQ Section 2, Schedule of Events.

5.3.2 Respondent presentations are only open to the invited Respondent, Proposal Evaluation Team members, the Solicitation Coordinator, and any technical consultants who are selected by the State to provide assistance to the Proposal Evaluation Team.

5.3.3 Oral presentations provide an opportunity for Respondents to explain and clarify their responses. Respondents must not materially alter their responses and presentations will be limited to addressing the items detailed in RFQ Attachment s A, B, and C, Technical Response & Evaluation Guides. Respondent pricing shall not be discussed during oral presentations. Evaluators may adjust Respondents' Technical Response scores based on Oral Presentations.

5.3.4 The State will maintain an accurate record of each Respondent's oral presentation session. The record of the Respondent's oral presentation shall be available for review

when the State opens the procurement files for public inspection.

5.4. Cost Proposals: The Cost Proposal containing the lowest cost will receive the maximum number of points per each section. See RFQ Attachment E, Cost Proposal & Evaluation Guide.

5.5. Clarifications and Negotiations: The State reserves the right to award a contract on the basis of initial responses received; therefore, each response should contain the respondent's best terms from a technical and cost standpoint. However, the State reserves the right to conduct clarifications or negotiations with respondents. All communications, clarifications, and negotiations shall be conducted in a manner that supports fairness in response improvement.

5.5.1 Clarifications: The State may identify areas of a response that may require further clarification or areas in which it is apparent that there may have been miscommunications or misunderstandings as to the State's specifications or requirements. The State may seek to clarify those issues identified during one or multiple clarification round(s). Each clarification sought by the State may be unique to an individual respondent.

5.5.2 Negotiations: The State may elect to negotiate with Qualified Respondents, within the competitive range, by requesting revised responses, negotiating costs, or finalizing contract terms and conditions. The State reserves the right to conduct multiple negotiation rounds.

5.5.2.1 Cost Negotiations: All responsive respondents within the competitive range will be given equivalent information with respect to cost negotiations. All cost negotiations will be documented for the procurement file. Additionally, the State may conduct target pricing and other goods or services level negotiations. Target pricing may be based on considerations such as current pricing, market considerations, benchmarks, budget availability, or other methods that do not reveal individual respondent pricing. During target price negotiations, respondents are not obligated to meet or beat target prices, but will not be allowed to increase prices.

5.5.2.2 If the State determines costs and contract finalization discussions and negotiations are not productive, the State reserves the right to bypass the apparent best evaluated Respondent and enter into contract negotiations with the next apparent best evaluated Respondent.

5.6. Evaluation Guide

The State will consider qualifications, experience, technical approach, and cost (if applicable) in the evaluation of responses and award points in each of the categories detailed below. The maximum evaluation points possible for each category are detailed below.

Evaluation Category	Maximum Points Possible
Mandatory Requirements (refer to RFQ Attachment A)	Pass/Fail
General Qualifications, Experience (refer to RFQ Attachment B)	20
Technical Qualifications & Approach (refer to RFQ Attachment C)	40
Oral Presentation (refer to RFQ Attachment D)	10
Cost Proposal (refer to RFQ Attachment E)	30

5.7. Contract Award

5.7.1. The Solicitation Coordinator will submit the Evaluation Team determinations and response scores to the head of the contracting agency, or the agency head's designee, for consideration along with any other relevant information that might be available and pertinent to contract award.

5.7.2. The contracting agency head, or the agency head's designee, will determine the apparent best-evaluated response. (To effect a contract award to a Respondent other than the one receiving the highest evaluation score, the head of the contracting agency must provide written justification and obtain written approval of the Chief Procurement Officer and the Comptroller of the Treasury.)

5.7.3. The State reserves the right to make an award without further discussion of any response.

5.7.4. The State will issue an Evaluation Notice and make the RFQ files available for public inspection at the time and date specified in the RFQ §2, Schedule of Events.

NOTICE: The Evaluation Notice shall not create rights, interests, or claims of entitlement in either the Respondent identified as the apparent best evaluated or any other Respondent.

5.7.5. The Respondent identified as offering the apparent best-evaluated must sign a contract drawn by the State pursuant to this RFQ. The contract shall be substantially the same as the RFQ Attachment H, *Pro Forma* contract. The Respondent must sign said contract no later than the Respondent Contract Signature Deadline detailed in RFQ § 2, Schedule of Events. If the Respondent fails to provide the signed contract by the deadline, the State may determine the Respondent is non-responsive to this RFQ and reject the response.

5.7.6. Notwithstanding the foregoing, the State may, at its sole discretion, entertain limited negotiation prior to contract signing and, as a result, revise the *Pro Forma* contract terms and conditions or performance requirements in the State's best interests, PROVIDED THAT such revision of terms and conditions or performance requirements shall NOT materially affect the basis of response evaluation or negatively impact the competitive nature of the RFQ and vendor selection process.

5.7.7. If the State determines that a response is nonresponsive and rejects it after opening Cost Proposals, the Solicitation Coordinator will re-calculate scores for each remaining responsive Cost Proposal to determine (or re-determine) the apparent best-evaluated response.

TECHNICAL RESPONSE & EVALUATION GUIDE

All Respondents must address all items detailed below and provide, in sequence, the information and documentation as required (referenced with the associated item references). All Respondents must also detail the response page number for each item in the appropriate space below.

The Solicitation Coordinator will review all responses to determine if the Mandatory Requirement Items are addressed as required and mark each with pass or fail. For each item that is not addressed as required, the Evaluation Team must review the responses and attach a written determination. In addition to the Mandatory Requirement Items, the Solicitation Coordinator will review each response for compliance with all RFQ requirements.

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	**Item Ref.**	**Section A— Mandatory Requirement Items**	**Pass/Fail**
		The Technical Response must be delivered to the State no later than the Technical Response Deadline specified in the RFQ § 2, Schedule of Events.	
		The Technical Response must not contain cost or pricing information of any type.	
		The Technical Response must not contain any restrictions of the rights of the State or other qualification of the response.	
		A Respondent must not submit alternate responses.	
		A Respondent must not submit multiple responses in different forms (as a prime and a subcontractor).	
	A.1.	Provide the Statement of Certifications and Assurances (RFQ Attachment F) completed and signed by an individual empowered to bind the Respondent to the provisions of this RFQ and any resulting contract. The document must be signed without exception or qualification.	
	A.2.	Provide a statement, based upon reasonable inquiry, of whether the Respondent or any individual who shall perform work under the contract has a possible conflict of interest (e.g., employment by the State of Tennessee) and, if so, the nature of that conflict. NOTE: Any questions of conflict of interest shall be solely within the discretion of the State, and the State reserves the right to cancel any award.	
	A.3.	Provide a current bank reference indicating that the Respondent's business relationship with the 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.	

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	**Item Ref.**	**Section A— Mandatory Requirement Items**	**Pass/Fail**
	A.4.	Provide two current positive credit references from vendors with which the Respondent has done business written in the form of standard business letters, signed, and dated within the past four (4) months.	
	A.5.	Provide an official document or letter from an accredited credit bureau, verified and dated within the last three (3) months and indicating a positive credit rating for the Respondent (NOTE: A credit bureau report number without the full report is insufficient and will not be considered responsive).	
	A.6.	Provide a valid, Certificate of Insurance that is verified and dated within the last six (6) months and which details all of the following: (a) Insurance Company (b) Respondent's Name and Address as the Insured (c) Policy Number (d) The following minimum insurance coverage: (i) Workers' Compensation/ Employers' Liability (including all states coverage) with a limit not less than the relevant statutory amount or one million Dollars ($1,000,000) per occurrence for employers' liability; (ii) Comprehensive Commercial General Liability (including personal injury & property damage, premises/operations, independent contractor, contractual liability and completed operations/products) with a bodily injury/property damage combined single limit not less than one million Dollars ($1,000,000) per occurrence two million Dollars ($2,000,000) aggregate; (e) The following information applicable to each type of insurance coverage: (i) Coverage Description, (ii) Exceptions and Exclusions, (iii) Policy Effective Date, (iv) Policy Expiration Date, and (v) Limit(s) of Liability.	
	A.7.	Provide a completed "Appendix 2 – Functions and Technical Requirements, to the Attachment H Pro Forma Contract. Reference the "instruction" tab for completing the excel spreadsheet.	

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	**Item Ref.**	**Section A— Mandatory Requirement Items**	**Pass/Fail**
	A.8.	Provide written confirmation that the Project functions or functional equivalent detailed in the RFQ for Stage 1(a) will meet the TDA timeline. (See RFQ Attachment H *Pro Forma Contract* - item A.4)	
	A.9.	Provide written confirmation that the proposed solution will maintain all data at all times within the U.S.	
	A.10.	Provide written confirmation that the proposed solution will encrypt data as outlined. RFQ Attachment H - *Pro Forma Contract* - Item A.43. Encryption	
	A.11.	Provide written confirmation of the security certification as outlined in RFQ Attachment H - *Pro Forma Contract* - Item A.53. Security Certification, Accreditation Audit	
State Use – RFQ Coordinator Signature, Printed Name & Date:			

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION B: GENERAL QUALIFICATIONS & EXPERIENCE. The Respondent must address all items detailed 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. Evaluation Team members will independently evaluate and assign one score for all responses to Section B— General Qualifications & Experience Items.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
	B.1.	Detail the name, e-mail address, mailing address, telephone number, and facsimile number of the person the State should contact regarding the response.
	B.2.	Describe the Respondent's form of business (*i.e.*, individual, sole proprietor, corporation, non-profit corporation, partnership, limited liability company) and business location (physical location or domicile).
	B.3.	Detail the number of years the Respondent has been in business.
	B.4.	Briefly describe how long the Respondent has been performing the goods or services required by this RFQ.
	B.5.	Describe the Respondent's number of employees, client base, and location of offices.
	B.6.	Provide a statement of whether there have been any mergers, acquisitions, or sales of the Respondent within the last ten (10) years. If so, include an explanation providing relevant details.
	B.7.	Provide a statement of whether the Respondent or, to the Respondent's knowledge, any of the Respondent's employees, agents, independent contractors, or subcontractors, proposed to provide work on a contract pursuant to this RFQ, have been convicted of, pled guilty to, or pled *nolo contendere* to any felony. If so, include an explanation providing relevant details.
	B.8.	Provide a statement of whether, in the last ten (10) years, the Respondent has filed (or had filed against it) any bankruptcy or insolvency proceeding, whether voluntary or involuntary, or undergone the appointment of a receiver, trustee, or assignee for the benefit of creditors. If so, include an explanation providing relevant details.
	B.9.	Provide a statement of whether there is any material, pending litigation against the Respondent that the Respondent should reasonably believe could adversely affect its ability to meet contract requirements pursuant to this RFQ or is likely to have a material adverse effect on the Respondent's financial condition. If such exists, list each separately, explain the relevant details, and attach the opinion of

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		counsel addressing whether and to what extent it would impair the Respondent's performance in a contract pursuant to this RFQ. NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders such opinions.
	B.10.	Provide a statement of whether there is any pending or in progress Securities Exchange Commission investigations involving the Respondent. If such exists, list each separately, explain the relevant details, and attach the opinion of counsel addressing whether and to what extent it will impair the Respondent's performance in a contract pursuant to this RFQ. NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders such opinions.
	B.11.	Provide a brief, descriptive statement detailing evidence of the Respondent's ability to deliver the goods or services sought under this RFQ (*e.g.*, prior experience, training, certifications, resources, program and quality management systems, *etc*.).
	B.12.	Provide a narrative description of the proposed contract team, its members, and organizational structure along with an organizational chart identifying the key people who will be assigned to provide the goods or services required by this RFQ, illustrating the lines of authority, and designating the individual responsible for the completion of each task and deliverable of the RFQ.
	B.13.	Provide a personnel roster listing the names of key people who the Respondent will assign to perform tasks required by this RFQ along with the estimated number of hours that each individual will devote to the required tasks. Follow the personnel roster with a resume for each of the people listed. The resumes must detail the individual's title, education, current position with the Respondent, and employment history.
	B.14.	Provide a statement of whether the Respondent intends to use subcontractors to accomplish the work required by this RFQ, and if so, detail: (a) the names of the subcontractors along with the contact person, mailing address, telephone number, and e-mail address for each; (b) a description of the scope and portions of the work each subcontractor will perform; <u>and</u> (c) a statement specifying that each proposed subcontractor has expressly

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		assented to being proposed as a subcontractor in the Respondent's response to this RFQ.
	B.15.	Provide documentation of the Respondent's commitment to diversity as represented by the following: (a) Business Strategy. Provide a description of the Respondent's existing programs and procedures designed to encourage and foster commerce with business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises. Please also include a list of the Respondent's certifications as a diversity business, if applicable. (b) Business Relationships. Provide a listing of the Respondent's current contracts with business enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises. Please include the following information: (i) contract description; (ii) contractor name and ownership characteristics (*i.e.*, ethnicity, gender, Tennessee service-disabled); and (iii) contractor contact name and telephone number. (c) Estimated Participation. Provide an estimated level of participation by business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises if a contract is awarded to the Respondent pursuant to this RFQ. Please include the following information: (i) a percentage (%) indicating the participation estimate. (Express the estimated participation number as a percentage of the total estimated contract value that will be dedicated to business with subcontractors and supply contractors having such ownership characteristics only and **DO NOT INCLUDE DOLLAR AMOUNTS**); (ii) anticipated goods or services contract descriptions; (iii) names and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veterans) of anticipated subcontractors and supply contractors. NOTE: In order to claim status as a Diversity Business Enterprise under this contract, businesses must be certified by the Governor's Office of Diversity Business Enterprise (Go-DBE). Please visit the Go-DBE website at https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&XID=9265 for more information. (d) Workforce. Provide the percentage of the Respondent's total current employees by ethnicity and gender.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		NOTE: Respondents that demonstrate a commitment to diversity will advance State efforts to expand opportunity to do business with the State as contractors and subcontractors. Response evaluations will recognize the positive qualifications and experience of a Respondent that does business with enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises and who offer a diverse workforce.
	B.16.	Provide a statement of whether or not the Respondent has any current contracts with the State of Tennessee or has completed any contracts with the State of Tennessee within the previous five-year period. If so, provide the following information for all current and completed contracts: (a) the name, title, telephone number and e-mail address of the State contact responsible for the contract at issue; (b) the name of the procuring State agency; (c) a brief description of the contract's specification for goods or scope of services; (d) the contract term; and (e) the contract number. NOTES: ▪ Current or prior contracts with the State are <u>not</u> a prerequisite and are <u>not</u> required for the maximum evaluation score, and the existence of such contracts with the State will <u>not</u> automatically result in the addition or deduction of evaluation points. ▪ Each evaluator will generally consider the results of inquiries by the State regarding all contracts responsive to Section B.16 of this RFQ.
	B.17.	Provide customer references from individuals who are <u>not</u> current or former State employees for projects similar to the goods or services sought under this RFQ and which represent: ▪ two (2) accounts Respondent currently services that are similar in size to the State; <u>and</u> ▪ three (3) completed projects. Reference from at least three (3) different individuals are required to satisfy the requirements above, e.g., an individual may provide a reference about a completed project and another reference about a currently services account. The standard reference questionnaire, which <u>must</u> be used and completed is provided at RFQ Attachment G. References that are not completed as required may be deemed nonresponsive and may not be considered. The Respondent will be <u>solely</u> responsible for obtaining fully completed reference questionnaires and including them in the Respondent's sealed Technical Response. In order to obtain and submit the completed reference questionnaires

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		follow the process below: (a) Add the Respondent's name to the standard reference questionnaire at Attachment G and make a copy for each reference. (b) Send a reference questionnaire and a new standard #10 envelope to each reference. (c) Instruct the reference to: (i) complete the reference questionnaire; (ii) sign <u>and</u> date the completed reference questionnaire; (iii) seal the completed, signed, and dated reference questionnaire within the envelope provided; (iv) sign his or her name in ink across the sealed portion of the envelope; and (v) return the sealed envelope directly to the Respondent (the Respondent may wish to give each reference a deadline, such that the Respondent will be able to collect all required references in time to include them within the sealed Technical Response). (d) <u>Do NOT open the sealed references upon receipt</u>. (e) Enclose all <u>sealed</u> reference envelopes within a larger, labeled envelope for inclusion in the Technical Response as required. NOTES: ▪ The State will not accept late references or references submitted by any means other than that which is described above, and each reference questionnaire submitted must be completed as required. ▪ The State will not review more than the number of required references indicated above. ▪ While the State will base its reference check on the contents of the sealed reference envelopes included in the Technical Response package, the State reserves the right to confirm and clarify information detailed in the completed reference questionnaires, and may consider clarification responses in the evaluation of references. ▪ The State is under <u>no</u> obligation to clarify any reference information.
	B.18.	Provide a statement and any relevant details addressing whether the Respondent is any of the following: (a) is presently debarred, suspended, proposed for debarment, or voluntarily excluded from covered transactions by any federal or state department or agency; (b) has within the past three (3) years, been convicted of, or had a civil judgment rendered against the contracting party from commission of fraud, or a criminal offence in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; (c) is presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed above; and has within a three (3) year period preceding the contract had one or more public transactions (federal, state, or local) terminated for cause or default.
	B.19.	Provide a list of any non-State standard products the Contractor may require which deviates from the State's Technology Architecture Product Standards document.
	B.20.	The State is amenable to making changes to RFQ Attachment H, *Pro Forma* contract. The State will take all reasonable suggested alternative or supplemental contract language changes by Respondents under advisement during the evaluation and post award processes, subject to any mandates or restrictions imposed on the State by applicable state or federal law. The State, however, recommends that Respondents include with their response any alternative or supplemental suggested contract language that a Respondent would propose. Clearly indicate, by providing a "red-line" of RFQ Attachment H, *Pro Forma* contract, all suggested alternative or supplemental contract language. Do not include any exceptions or changes that (1) contradict a Federal requirement or a Mandatory Requirement, or (2) push back any deadlines.
SCORE *(for all Section B—Qualifications & Experience Items above)* : *(maximum possible score = 20)*		
State Use – Evaluator Identification:		

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION C: TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH. The Respondent should explain its approach to providing goods or services to the State. The items listed below represent specific questions the State would request you answer in your response. For ease of review, please annotate your explanation so that it contains references to the items listed below where they are addressed. Respondent should not feel constrained to answer only the specific questions listed below in its explanation and should feel free to provide attachments if necessary in an effort to provide a more thorough response.

The Evaluation Team, made up of three (3) 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 scores 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**
Technical					
	C.1.	Provide a narrative that illustrates the Respondent's understanding of the State's requirements and project schedule.		**25**	
	C.2.	Provide a narrative that illustrates how the Respondent will complete the delivery of goods or scope of services, accomplish required objectives, and meet the State's project schedule.		**15**	
	C.3.	Provide a narrative that illustrates how the Respondent will manage the project, ensure delivery of specified goods or completion of the scope of services, and accomplish required objectives within the State's project schedule.		**25**	
	C.4.	Describe your company's approach to meet project deliverables and **required milestones** to satisfy mandatory implementation timeframe based on the defined scope and requirements RFQ		**25**	

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	**Item Ref.**	**Section C— Technical Qualifications, Experience & Approach Items**	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
		Attachment H - *Pro Forma* – Item A.4. **NOTE:** Do not include any pricing or cost structures.			
	C.5.	Provide a narrative that illustrates how the Respondent will complete the delivery of **Applications, Permits, and Renewals requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**50**	
	C.6.	Provide a narrative that illustrates how the Respondent will complete the delivery **of Billing and Fee collection requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**50**	
	C.7.	Provide a narrative that illustrates how the Respondent will complete the delivery of **Inspection Management requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**50**	
	C.8.	Provide a narrative that illustrates how the Respondent will complete the **Violation Tracking requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**25**	
	C.9.	Provide a narrative that illustrates how the Respondent will complete the **Complaint Tracking requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**25**	
	C.10.	Provide a narrative that illustrates how the Respondent will complete the **Mobile Access requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**35**	

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.11.	Provide a narrative that illustrates how the Respondent will complete the **System Common requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**35**	
	C.12.	Provide a narrative that illustrates how the Respondent will complete **Performance Data Analysis requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**35**	
	C.13.	Provide a narrative that illustrates how the Respondent will complete the **Certification Testing and Administration requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**20**	
	C.14.	Provide a narrative that illustrates how the Respondent will complete the **System Use Training requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements* and RFQ Attachment G - *Pro Forma* - Item A.17.		**5**	
	C.15.	Provide a narrative that illustrates the Respondent understands the **State's Project Management Methodology requirements** RFQ Attachment H - *Pro Forma* – Item A.3.		**10**	
	C.16.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Organizational Change Management (OCM) requirements** as described in RFQ Attachment H - *Pro Forma* – Item A.16 and RFQ Attachment G - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 4.		**10**	

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.17.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Project Initiation Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 1. Also provide draft/example of Turnover/Transition Plan as described in Attachment H - *Pro Forma* – Item A.69.		**10**	
	C.18.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Project Management Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 2.		**10**	
	C.19.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Business Process Re-engineering Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 3.		**10**	
	C.20.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Design Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 5.		**20**	
	C.21.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Development Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 6.		**20**	
	C.22.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Acceptance Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 7.		**10**	

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.23.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Implementation Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 8.		**10**	
	C.24.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **TDA Staff Training Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 9.		**5**	
	C.25.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **TDA Staff Training Estimates** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 10.		**5**	
	C.26.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Maintenance and Support requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 11.		**15**	
	C.27.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **System Warranty of System Products/Services requirements** as described in RFQ Attachment H - *Pro Forma* - Item A.18.		**10**	
	C.28.	Provide a narrative that describes the customary division of support between the vendor and the customer. Include standard roles and responsibilities definitions for both the vendor and the customer for new application releases, upgrades, and administrative functions.		**5**	

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.29.	Provide a narrative that describes the customary product maintenance and enhancement cycle.		**10**	
	C.30.	Provide a narrative that describes the process involved in implementing your product for a new customer of similar size and scope of implementation as the State is envisioning.		**25**	
	C.31.	Provide a narrative that describes the additional support services provided. Do not include ANY pricing in response to this question.		**10**	
	C.32.	Provide a narrative that describes the **staffing requirements to be met by the State** in order to meet the schedule as described in RFQ Attachment H - *Pro Forma* - Item A.7. Provide a description of the skills required and the quantities and levels of commitment for each skill.		**5**	
	C.33.	Provide a narrative that illustrates how the Respondent how the Respondent has completed the delivery of a Mobile solution, in a similar size project Describe your experience in implementation including the following: • *How long has the Mobile solution been in production?* • *How many implementations in the past 5 years included a mobile solution?* • *Provide the type and number of mobile clients.* ***Client information:*** • *Type of client (e.g. government entity (local, State, Federal), private company etc.);* • *Number of back-office users;*		**20**	

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	**Item Ref.**	**Section C— Technical Qualifications, Experience & Approach Items**	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
		• *Number of licensees with online accounts;* • *Total number of licensees;* • *Number of license types;* • *Number of locations;* • *Number of licensing entities;* • *Annual licensing revenues; and* • *Any other information relevant to describing the client organization(s) in the context of this Competitive Negotiation* ***Project information:*** • *Project including original estimates and final budget* • *Project duration including start/end dates; including original estimates and final project duration.* • *Number of Contractor staff (Full Time Employees) involved in the implementation; and* • *Number of client staff (FTEs) involved in the implementation.*			
	C.34.	Provide a narrative that Illustrates how the proposed system will provide a **Third Party Cashiering System not excluding the State Authorized Card Credit Card processor, and the State's cashiering system (iNovah)** as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common – System Interface. Appendix 2 – Bill & Fee Collection – Fees and Fines Collection Appendix 2 – Bill & Fee Collection – On-line Payment.		**5**	
	C.35.	Provide a narrative that illustrates how the proposed system will provide **Document Management**, to include scanning, uploading, attaching, document metadata, document lookup/retrieval, document retention, document archiving, version control, etc. as defined in RFQ Attachment H - *Pro Forma* - Item A.56.		**20**	

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.36.	Provide a narrative that Illustrates how the proposed system will provide **interface methods and tools with other non TDA systems** (i.e. State's USALIMS system, Third party Lab results, Revenue, etc.) as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	
	C.37.	Provide a narrative that Illustrates how the proposed system will **provide electronic signature** as defined in RFQ Attachment H - *Pro Forma* – Appendix 2 – Applications, Permits & Renewal – License Application. Appendix 2– Mobile Access.		**5**	
	C.38.	Provide a narrative that Illustrates how the proposed system will provide **compliance with Payment Card Industry (PCI) and 508 Compliance requirements** as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common - Security.		**5**	
	C.39.	Provide a narrative that Illustrates how the proposed system will **provide automated business rules** as required in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	
	C.40.	Provide a narrative that Illustrates how the proposed system will **provide system notifications** - via text message or emails as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	
	C.41.	Provide a narrative that Illustrates how the proposed system will provide **audit trail functionality** to track the details of all events that occur within the system including any addition, change, or deletion of data as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	

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.42.	Provide a narrative detailing how the contractor will develop detailed **system documentation** described in RFQ Attachment H - *Pro Forma* - Item A.21. System documentation differs from training materials in that it defines the system architecture, explains project implementation activities, and demonstrates how the system can be tailored over time to fit evolving needs of the State.		**5**	
	C.43.	Provide a narrative detailing how well your **Help Desk** processes match the business needs outlined in RFQ Attachment H - *Pro Forma* – Item A.22.. Specifically address each sub section: hours of operation, communication methods, level of staff knowledge, and incident resolution procedures.		**10**	
	C.44.	Describe (without revealing cost) the **User Licensing**, including any Third Party software, necessary to support the System, the types of licenses and numbers of license necessary to support all users, disaster recovery, and non-production environments, including training in RFQ Attachment H - *Pro Forma* - Item A.23.		**10**	
	C.45.	Provide a narrative detailing your network architectural design “without revealing proprietary details or trade secrets.”		**5**	

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.46.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections: A.34. Legal Compliance A.36. Miscellaneous Security Provisions (including who is doing the scans) A.41. Data Ownership A.42. Data Location A.44. Import and Export of Data A.68. Termination or Suspension of Service A.69. Turnover Plan A.75. Data and System Conversion		**30**	
	C.47.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections: A.39. Protection of Information		**10**	
	C.48.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections: A.43. Encryption		**10**	
	C.49.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections A.45. Data Protection A.46. Industry Data Security Standard		**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)*	

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	**Item Ref.**	**Section C— Technical Qualifications, Experience & Approach Items**	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
Total Raw Weighted Score / **Maximum Possible Raw Weighted Score** *(i.e., 5 x the sum of item weights above)*			**X 40** *(maximum possible score)*	**= SCORE:**	
State Use – Evaluator Identification:					
State Use – Solicitation Coordinator Signature, Printed Name & Date:					

TECHNICAL RESPONSE & EVALUATION GUIDE

Attachment D: ORAL PRESENTATION. The Respondent must address ALL Oral Presentation Items (below).

A Proposal Evaluation Team, made up of three or more State employees, will independently evaluate and score the presentation 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:			
Oral Presentation Items	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
D.1. Demo Application, License/Permits & Renewals		**5**	
D.2. Demo Inspections (mobile devices online/offline, assigning inspections to inspectors, etc)		**5**	
D.3 Demo Bill and Fee Collections		**5**	
D.4 Demo Third Party Laboratory lab results transferred into system		**2**	
D.5 Demo setting up a new user		**2**	
D.6 Demo Document Management Capabilities		**5**	
D.7 Demo Certification Testing and Administration		**4**	
D.8 Demo rule based alerts		**3**	
D.9 Demo maintaining business rules in the system		**5**	
D.10 Describe lessons learned regarding migrating current date into the new system		**3**	
D.11 Describe the Organizational Change that has occurred with business processes, job roles, and organizational structure with the implementation of the system		**5**	
Total Raw Weighted Score *(sum of Raw Weighted Scores above)***:** The Solicitation Coordinator will use this sum and the formula below to calculate the score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.			

RESPONDENT LEGAL ENTITY NAME:	

total raw weighted score / **maximum possible raw weighted score** *(i.e., 5 x the sum of item weights above)*	**X 10** *(maximum section score)*	**= SCORE:**	

State Use – Evaluator Identification:
State Use – Solicitation Coordinator Signature, Printed Name & Date:

Cost Proposal & Evaluation 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 the delivery of specified goods for the entire scope of services including all services defined in the Scope of Services of the RFQ Attachment H, *Pro Forma* Contract and for the entire contract period. The Cost Proposal shall remain valid for at least 120 days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract resulting from this RFQ. All monetary amounts shall be in U.S. currency and limited to two (2) places to the right of the decimal point.

NOTICE: The Evaluation Factor associated with each line item of cost 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 line item of costs herein, pursuant to the second paragraph of the *pro forma* contract section C.1. (refer to RFQ Attachment H), "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 entity responding to the provisions of this RFQ and any contract awarded pursuant thereto. If said individual is not responding in an individual capacity or is the *President* or *Chief Executive Officer*, this document must attach evidence showing the individual's authority to legally bind the entity responding to this RFQ.

RESPONDENT SIGNATURE:	
PRINTED NAME & TITLE:	
DATE:	

RESPONDENT LEGAL ENTITY NAME:		
Cost Item Description **(Cost for all Stages – see RFQ attachment H – item-A.4)**	**Proposed Cost** **DDI through Retainage Period**	**State Use ONLY**
1. Design, Development, and Implementation (DDI)	$	
2. Post-Implementation Support and Maintenance (Stage 1 through Retainage)	$	
3. Post-Implementation Hosting (Stage 1 through Retainage)	$	
The RFQ Coordinator will use this sum and the formula below to calculate the Part A Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations	**Total System Cost** **(Part A Evaluation Cost Amount):** *(Sum of Proposed Costs Above)*	
Lowest Part A Evaluation Cost Amount from <u>all</u> Proposals **Part A Evaluation Cost Amount Being Evaluated**	**x 20** *(maximum section score)* **= PART A SCORE:**	
State Use ONLY – RFQ Coordinator Signature, Printed Name & Date:		

RESPONDENT LEGAL ENTITY NAME:									
Recurring Annual Costs for Hosting, Support and Maintenance. **(Please list the cost post retainage period. The State will sum rows and record the sum in the "State Use Only" column.)**	**Proposed Cost - Hosting, Support and Maintenance (Post Retainage)**								**State Use ONLY**
	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Optional Year 1**	**Optional Year 2**	**Optional Year 3**	**Evaluation Cost**
Hosting (includes 250 User Licensing for TDA users)	$	$	$	$	$	$	$	$	
Support and Maintenance	$	$	$	$	$	$	$	$	
User Licensing Fee for each additional 10 TDA users post retainage period.	$	$	$	$	$	$	$	$	
The RFQ Coordinator will use this sum and the formula below to calculate the Part B Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.								**Part B Evaluation Cost Amount:** *(Sum of Evaluation Costs Above)*	
Lowest Part B Evaluation Cost Amount from all Proposals / **Part B Evaluation Cost Amount being evaluated**				**x 8** *(maximum section score)*				**= PART B SCORE:**	
State Use ONLY – RFQ Coordinator Signature, Printed Name & Date:									

RESPONDENT LEGAL ENTITY NAME:	

CHANGE ORDER RATES SCHEDULE

The hourly change order rates, detailed below, shall indicate the proposed rates for processing all State-approved additional work. All monetary amounts are United States currency.

NOTE: The costs proposed must be fully loaded to cover travel, meals, and lodging expenses associated with providing the services; the State will not pay travel-related expenses separately.

The Proposer may enter zero (0) in a required Proposed Hourly Rate cell; however, the Proposer must not leave any required Proposed Rate cell blank. For evaluation and contractual purposes, the State shall interpret a blank Proposed Rate cell as zero (0).

NOTE: In Contract Section C.3.c, there is a seven percent (7 %) cap on the total amount of Additional Work that can be procured without amending the contract for additional funds. However, this cap is for contractual purposes only and does not apply to, or in any way restrict, the change order amounts that the vendor may propose below.

Cost Item Description	**Proposed Cost**	**State Use ONLY**	
		Evaluation Factor ***(Note: Actual usage is unknown. The evaluation factors below are estimated usage for cost evaluation only.)**	**Evaluation Cost** **(cost x factor)**
Project Manager	$ /HOUR	150	
Business Analyst	$ /HOUR	200	
Technical Manager/Lead	$ /HOUR	400	
Developer	$ /HOUR	800	
The RFQ Coordinator will use this sum and the formula below to calculate the Part C Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.		**Part C Evaluation Cost Amount:** *(Sum of Evaluation Costs Above)*	

Lowest Part C Evaluation Cost Amount from all Proposals / **Part C Evaluation Cost Amount being evaluated**	**x 2** *(maximum section score)*	**= PART C SCORE:**	
FINAL SCORE (TOTAL OF PART A, PART B, AND PART C):			

State Use ONLY – RFQ Coordinator Signature, Printed Name & Date:

STATEMENT OF CERTIFICATIONS AND ASSURANCES

An individual responding in his or her individual capacity or legally empowered to contractually bind the Respondent must complete and sign the Statement of Certifications and Assurances below as required, and this signed statement must be included with the response as required by the Request for Qualifications.

The Respondent does, hereby, expressly affirm, declare, confirm, certify, and assure ALL of the following:

1. The Respondent will comply with all of the provisions and requirements of the RFQ.
2. The Respondent will provide all specified goods or services as required by the contract awarded pursuant to this RFQ.
3. The Respondent accepts and agrees to all terms and conditions, except changes as set forth in the response (refer to RFQ Attachment B, Item B#20), set out in the RFQ Attachment H, *pro forma* Contract.
4. The Respondent awarded the Contract resulting from this RFQ shall accept the State Purchasing Card ("P-Card") as a form of payment at no cost to the State.
5. The Respondent acknowledges and agrees that a contract resulting from the RFQ shall incorporate, by reference, all Respondent's responses as a part of the contract.
6. The Respondent will comply, as applicable, with:
   (a) the laws of the State of Tennessee;
   (b) Title VI of the federal Civil Rights Act of 1964;
   (c) Title IX of the federal Education Amendments Act of 1972;
   (d) the Equal Employment Opportunity Act and the regulations issued there under by the federal government; and,
   (e) the Americans with Disabilities Act of 1990 and the regulations issued there under by the federal government.
7. To the best of the undersigned's knowledge, information or belief, the information detailed within the Response to the RFQ is accurate.
8. The Response submitted to the RFQ was independently prepared, without collusion, and under penalty of perjury.
9. No amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Respondent in connection with the request or any potential resulting contract.
10. Both the Technical Response and the Cost Proposal submitted in response to the RFQ shall remain valid for at least 120 days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract pursuant to the RFQ.

By signature below, the signatory certifies legal authority to bind the responding entity to the provisions of this request and any contract awarded pursuant to it. The State may, at its sole discretion and at any time, require evidence documenting the signatory's authority to be personally bound or to legally bind the responding entity.
DO NOT SIGN THIS DOCUMENT IF YOU ARE NOT LEGALLY AUTHORIZED TO DO SO BY THE ENTITY RESPONDING TO THIS RFQ.

SIGNATURE & DATE: _____

PRINTED NAME & TITLE: _____

LEGAL ENTITY NAME: _____

FEIN or SSN: _____

REFERENCE QUESTIONNAIRE

The standard reference questionnaire provided on the following pages of this attachment MUST be completed by all individuals offering a reference for the Respondent.

The Respondent will be responsible for obtaining completed reference questionnaires as required (refer to RFQ Attachment B, General Qualifications & Experience Items, Item B.17.), and for enclosing the sealed reference envelopes within the Respondent's Technical Proposal.

RFQ # 32505-00215 REFERENCE QUESTIONNAIRE

RESPONDENT NAME: RESPONDENT NAME (completed by respondent before reference is requested)

The "respondent name" specified above, intends to submit a response to the State of Tennessee in response to the Request for Qualifications (RFQ) indicated. As a part of such response, the respondent must include a number of completed and sealed reference questionnaires (using this form).

Each individual responding to this reference questionnaire is asked to follow these instructions:

- complete this questionnaire (either using the form provided or an exact duplicate of this document);
- sign and date the completed questionnaire;
- seal the completed, signed, and dated questionnaire in a new standard #10 envelope;
- sign in ink across the sealed portion of the envelope; and
- return the sealed envelope containing the completed questionnaire directly to the respondent.

(1) What is the name of the individual, company, organization, or entity responding to this reference questionnaire?

(2) Please provide the following information about the individual completing this reference questionnaire on behalf of the above-named individual, company, organization, or entity.

NAME:	
TITLE:	
TELEPHONE #	
E-MAIL ADDRESS:	

(3) What goods or services do/did the vendor provide to your company or organization?

RFQ # 32505-00215 PROPOSAL REFERENCE QUESTIONNAIRE — PAGE 2

(4) What is the level of your overall satisfaction with the vendor of the goods or services described above?

Please respond by circling the appropriate number on the scale below.

	1	2	3	4	5	
least satisfied						**most satisfied**

If you circled 3 or less above, what could the vendor have done to improve that rating?

(5) If the goods or services that the vendor provided to your company or organization are completed, were the goods or services completed in compliance with the terms of the contract, on time, and within [insert something here]? If not, please explain.

(6) If the vendor is still providing goods or services to your company or organization, are these goods or services being provided in compliance with the terms of the contract, on time, and within [insert something here]? If not, please explain.

(7) How satisfied are you with the vendor's ability to perform based on your expectations and according to the contractual arrangements?

(8) In what areas of goods or service delivery do/did the vendor excel?

RFQ # 32505-00215 PROPOSAL REFERENCE QUESTIONNAIRE — PAGE 3

(9) In what areas of goods or service delivery do/did the vendor fall short?

(10) What is the level of your satisfaction with the vendor's project management structures, processes, and personnel?

Please respond by circling the appropriate number on the scale below.

	1	2	3	4	5	
least satisfied						**most satisfied**

What, if any, comments do you have regarding the score selected above?

(11) Considering the staff assigned by the vendor to deliver the goods or services described in response to question 3 above, how satisfied are you with the technical abilities, professionalism, and interpersonal skills of the individuals assigned?

Please respond by circling the appropriate number on the scale below.

	1	2	3	4	5	
least satisfied						**most satisfied**

What, if any, comments do you have regarding the score selected above?

(12) Would you contract again with the vendor for the same or similar goods or services?

RFQ # 32505-00215 PROPOSAL REFERENCE QUESTIONNAIRE — PAGE 4

Please add any additional comments to the response above.

REFERENCE SIGNATURE:
(by the individual completing this request for reference information)

_____
(must be the same as the signature across the envelope seal)

DATE:

_____

RFQ # 32505-00215 PRO FORMA CONTRACT

The *Pro Forma* contract detailed in following pages of this exhibit contains some “blanks” (signified by descriptions in capital letters) that will be completed with appropriate information in the final contract resulting from the RFQ.

***PRO FORMA* CONTRACT**

BETWEEN THE STATE OF TENNESSEE,
TENNESSEE DEPARTMENT OF AGRICULTURE
AND
CONTRACTOR NAME

This Contract, by and between the State of Tennessee, **Tennessee Department of Agriculture** ("State") and *Contractor Legal Entity Name* ("Contractor"), is for the provision of obtaining the software, implementation services, hosting and ongoing support the Consumer Industry Service Division's licensing, permitting, inspection, and education as further defined in the "SCOPE". State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is a/an Individual, For-Profit Corporation, Non-Profit Corporation, Special Purpose Corporation Or Association, Partnership, Joint Venture, Or Limited Liability Company.
Contractor Place of Incorporation or Organization: Location
Contractor Edison Registration ID # Number

A. SCOPE OF SERVICES:

A.1. The Contractor shall provide all service and deliverables as required, described, and detailed herein and shall meet all service and delivery timelines as specified by this Contract.

A.2. <u>Summary of Services.</u>

Through this contract, the State shall obtain an enterprise computer software system that shall : encompasses replacement of the current TDA regulatory system(s), including but not limited to comprehensive project management, business and system analysis, provision of package software, software customization, development of system interfaces, testing, training, system implementation, hosting, support, and maintenance.

Under the terms of this Contract, the Contractor shall develop the System to meet the requirements and to develop deliverables identified herein.

Appendix 1 – Glossary
Appendix 2 – Functional and Technical Requirements
Appendix 3 – Statistics
Appendix 4 – Reports
Appendix 5 – Forms
Appendix 6 – Contractor Requirements
Appendix 7 – State's Acceptable Use Policy and Acceptance Use Agreement
Appendix 8 – Non-disclosure Agreement (NDA)
Appendix 9 – Enterprise Information Security Policies
Appendix 10 – Deliverable Specification Sheet

The Contractor's responses to the appendices listed above shall bind the Contractor and become part of this Contract upon execution.

- The Contractor's obligations include: the Design, Development and Implementation (DDI) for the five project stages,
- The project includes hosting, support, and maintenance (HSM) during Stage 1, Stage 2, Stage 3, Stage 4, and Stage 5, followed by the 6-month warranty period after the approved implementation of Stage 5.
- Consecutive one-year hosting, support and maintenance periods, after the conclusion of the six-month retainage period at the TDA's discretion.

A.3. <u>Project Management.</u>

The State requires that the Contractor follow a systematic approach to the design, development, and implementation of the System to ensure that a comprehensive and expandable system is implemented. The State of Tennessee's Information Technology Project Management Methodology is Tennessee Business Solutions Methodology (TBSM). TBSM is based on the principles set forth by the Project Management Institute (PMI) and on industry best practices that are adapted to meet the state's needs. The table below provides a high level illustration of the TBSM project phases and activities included, but not limited to the standard project management templates, tasks and deliverables.

Tennessee Business Solutions Methodology

Pre-Engagement Phase	Project Initiation	Project Planning	Project Execution / Project Monitoring & Control	Project Closing
• Project Charter (initial draft) • Initial Project Assessment	• Project Charter • BA Approach • Requirements Mgmt Plan • BPI Plan • Process In , Diagrams & Desc Requirements Capabilities • Solution Approach	• Requirements Development Plan • Requirements Traceability Matrix • Project Mgmt Plan • Work Breakdown Structure • Activity List • Scope Statement	• Project Schedule • Risk Register • Status • Change Control • Communications • Training • Implementation	• Closing Documents • Project Evaluation • Lessons Learned

The Contractor will be required to utilize the TBSM model including the templates or a comparable project management methodology and accompanying template documents similar to the TBSM. In aligning with industry standards, The Tennessee Business Solutions Methodology (TBSM) encompasses many templates for use throughout the phases of project management.

The Contractor shall address all the Deliverables for the life-cycle phases in their project plan but can organize and plan for the accomplishment of the work based on their experience with projects of similar scale and scope. The complete TDA System detailed requirements, which identify the required functionality of the System, are provided in Contract Appendix 2 – Functional and Technical Requirements.

The Contractor shall define the overall Project Management approach for the project and should describe, in general terms, the roles and authorities of project team members from both the State staff and the Contract staff. The Project Management Approach should be based on the Contractors best practices and experience, and should be fully described in the section of the Project Management Plan. The Contractor confirms their commitment to meet all Project Management requirements resulting deliverables defined in this Section regardless of the approach proposed. Each subsection within the Contractor requirements provides a narrative on the requirements, followed by a table defining the tasks and Deliverables to be fulfilled by the Contractor.

The Contractor shall provide project Deliverables for the TDA System in the form and format agreed to by the State.

A.4. <u>Required Milestones</u>.

The implementation dates for the TDA system milestones are as follows:

TDA System Milestones	Description	Target Completion Date
Stage 1A	Those features and functions indicated in RFQ Attachment H - Appendix 2 as Stage 1A for the Food Safety, Petroleum, Weights & Measures programs	Go Live 03-1-16
Stage 1B	Those features and functions indicated in Appendix 2 as Stage 1B for the Food Safety, Dairy, Petroleum, Weights & Measures programs	Go Live 07-1-16
Stage 2	Ag Inputs - Feed, Seed, Fertilizer, Lime	Go Live 08-1-16
Stage 3	Plant Certification, Apiary	Go Live 10-1-16
Stage 4	Animal Health	Go Live 12-1-16
Stage 5	Pesticides	Go Live 02-1-17

A.5. Service Description.

The Contractor shall deliver the services and deliverables as described and detailed in *Pro Forma* Contract Appendix 6 — Contractor Requirements.

a. Kickoff Meeting and Presentation.

The Contractor shall participate in a State-led Kickoff Meeting. The purpose of the Kickoff Meeting shall be to introduce the Contractor to the State project stakeholders, and ensure agreement regarding project objectives, roles and responsibilities, strategy, and known risks. The contractor shall prepare and deliver a presentation for the kickoff meeting that synthesizes their approach to the overall project, provides high-level milestones, and introduces the Contractor team.

The Contractor Project Manager shall ensure timely and accurate submission of project management deliverables to the State Business Project Manager as listed below:

b. Project Initiation and Project Management Phase Requirements.

The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6, Tables 1 and 2.

Work Breakdown Structure (WBS) and Project Schedule lists the work packages to be performed for the project, and a schedule baseline that will be used as a reference point for managing project progress as it pertains to schedule and timeline

c. Weekly Status Report.

The Contractor shall prepare and submit to the State Business Project Manager a Weekly Status Report. The report shall contain a synopsis of the status of activities, outstanding issues and expected resolution dates, expended level of effort/burn rate, and key risks and issues. Items to be tracked in this report will include, at a minimum, open technical questions, requests for information, schedule of resources for the coming week, and requests for documentation.

The Contractor shall also report progress against the Project Schedule in the Weekly Status Report, including, at a minimum, an assessment of progress against plan, and details of slipping tasks. For any planned tasks that are not worked or completed during the reporting

period, the Contractor shall include an explanation of the failure to meet the schedule and detailed plans to overcome the failure and prevent its recurrence.

d. Monthly Progress Report.

The Contractor shall prepare and submit to the Project Steering Committee a Monthly Progress Report throughout the project's duration. Monthly Progress Reports shall contain, at a minimum:

i. Progress toward project milestones.
ii. Explanations of schedule and cost variances relative to the previous month's progress report and the baseline schedule and cost projections.
iii. Updates on implementation.
iv. Status of deliverables.
v. Action items and status.

e. Requirements Verification and Fit-Gap Analysis.

The Contractor shall work with State project team members, as identified by the State, to verify the requirements outlined in Contract Appendix 2 – Functional and Technical Requirements, and to map and document the extent that the Contractor's solution meets each requirement. The Contractor shall use its responses to Contract Appendix 2 – Functional and Technical Requirements, for the verification process. The Contractor shall document any necessary requirement changes or requirement gaps identified as a result of the requirements verification process.

f. Defect Tracking Log.

The Contractor shall develop and maintain a Defect Tracking Log which shall include at a minimum, for each Defect:

a. Unique tracking number.
b. Short name and description of the defect.
c. Reference to test condition that identified the defect.
d. Date Defect was identified.
e. Tester.
f. Disposition (e.g., Not a Defect, Fixed, Successfully Retested, etc.).
g. Severity Level.
h. Description of changes made to correct the defect.

g. Final Project Report.

The Contractor shall create a Final Project Report summarizing project activities, lessons learned, and recommended next steps. The Final Project Report shall be submitted to the State Business Project Manager no later than fifteen (15) business days prior to the Contract End Date. The State will provide written acceptance of the Final Project Report.

The Contractor shall prepare and deliver to the State for review and approval a Requirements Verification document that includes a finalized list of Business Requirements Specifications, which detail the specific features and functions of each requirement. The State will provide written acceptance of the Requirements Verification document.

Additionally, the Contractor shall provide other requirements as described in *Pro Forma* Contract, Appendix 6. An abbreviated listing of those items is detailed below.

a. Business Process Re-engineering.

The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 3.

b. Organizational Change Management.

The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 4.

c. System Design,
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 5.

d. System Development.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 6.

e. System Acceptance.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 7.

f. System Implementation.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 8.

g. Training.
Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Tables 9 and 10.

h. Maintenance & Support.
Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 11.

i. System Support & Warranty.
Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 12.

A.6. Business Process Re-engineering.
Certain State processes have been identified for re-engineering, based on the opportunity to achieve significant improvements, including:

- Manage, Process, and Track:
  - Applications, Permits & Renewal
  - Bill & Fee Collection
  - Inspection Management
  - Violation Tracking
  - Complaint Tracking
  - Mobile Access
  - System Common
  - Performance Data Analysis
  - Certification, Testing, and Training
  - System Use Training
- Ability of license process owners to easily design and create workflows within the System
- Customer service improvements (wait time reduction, better response to inquiries)
- Fraud reduction
- Efficiency and process cost reduction
- Customer web-based self-service
- Capturing and using the customer's e-mail and text addresses, using them to keep the customer up-to-date on the status of transactions, and reducing the number of customer service status calls to the State staff.
- Integration of content/document management services (i.e. accepting scanned customer documents at the State office or the customer's computer, attaching those documents to the State record, and using only the scanned images from that point forward.)

- Working closely with State applicants to initiate transactions through the web and eliminate paper in the process.
- Improved file search and reporting capabilities
- Integration with the State's e-payment service and State authorized payment card Vendor
- Interface with third-party entities

The Contractor shall create and deliver a full set of updated "To-Be" process flows that the Contractor recommends to modernize and streamline State license, permit, enforcement, training processes during the Design Stage.

A.7. State Project Team.

The State intends to commit needed internal resources in support of the successful and timely delivery of the System. During the Contract term, State staff will not report to Contractor staff, and Contractor staff shall not assign tasks to State staff. State staff will not be responsible for the completion of Contractor-assigned deliverables per this Contract. The State shall provide the following, in addition to other staff as needed.

a. State Project Manager.

The State Project Manager shall be the Contractor's point of contact for the Project. The State Project Manager shall be appointed and on-site at the State office on or before the Contract start date. The State Project Manager shall consult with the Project Steering Committee on a continuing basis in every stage of the Project. This joint effort shall ensure that the Project is properly implemented, supporting each program area's requirements, and properly documented. The State Project Manager shall provide expertise, assistance, and technical leadership in all Project matters, including but not limited to, policy, staffing and organization, environment, data, information processing, current systems, and acceptance testing. The State Project Manager shall work closely with the Contractor's Project Manager in day-to-day Project activities.

b. State Contract Administrator.

The State shall provide a Contract Manager who shall be responsible for ensuring that the Project is in compliance with the Contract and satisfies the State's requirements.

c. Other State Project Staff Assignments.

The State shall assign staff, according to the Project timeline, to key Project roles, as necessary, to participate with the Contractor's staff in all Project Management Processes and Project stages. At the State's discretion, State personnel may be substituted, added, or removed.

A.8. Contractor Project Team.

All employees of the Contractor, who shall perform Services under this contract, shall possess the necessary qualifications, training, licenses and permits as may be required within the contract.

a. Contractor's Key Project Staff.

Except as otherwise provided for herein, the Contractor agrees that the Key Project Staff (Project Manager, Business Analyst, Technical Manager/Lead, Lead Designer, Lead Trainer) will continue their assignment to completion of said assignment. The same individual may fill multiple roles.

The Contractors Project Manager shall be present on-site at critical points during the contract period and will be responsible for the day-to-day management of the project's timeline, personnel, and administration. The Project Manager's role shall include, but not be limited to, resource allocation, ensuring Contractor staff performance, ensuring the timely development, quality, and acceptance of implementation documents and all other Deliverables,

communicating with the Project Team, chairing the status meetings. The Contractor Project Manager will also be required, upon reasonable notice to meet with the State's Project Manager and other State and/or TDA executives when requested by the State's Project Manager. The Contractor's Project Manager shall always be able to be contacted through Final Acceptance of the TDA system

1. The Contractor understands that the confidence in the professional abilities of the State's approved Key Project Staff is a vital component to meet all requirements to successfully implement the TDA. Therefore, if the Contractor wishes to remove any of the approved Contractor's Key Project Staff from the project prior or after his or her commencement or during the assignment period, the Contractor shall first, before proceeding with such removal, consult with and seek the advice and opinion of the State Project Manager. If, after said consultation, it is mutually agreed that such a removal shall take place, the Contractor will promptly provide the resume of a recommended potential replacement having similar or better qualifications for the State Project Manager's review and approval. If the State Project Manager does not approve Contractor's recommended candidate, the Contractor will promptly provide additional candidates for the State Project Manager's review. If the State Project Manager still cannot agree to a replacement, the State Project Manager reserves the right to either (a) have Key Project Staff remain on the project, or (b) terminate this Contract for cause as indicated in *Pro Forma* Contract Section D.6. Upon State's Project Manager approval, the replacement will become Key project Staff and will be subject to the terms and condition of this Contract. If the Key Project Staff member's work has already commenced, the Contractor will ensure a smooth transition, including having the Contractor staff who is leaving train the replacement Contractor staff at the State's facilities (see Staff Transition Period below).

2. If the State Project Manager does not agree to the replacement of Key Project Staff and does not wish to terminate the Contract, the Key Project Staff member must remain on the Project and must continue to work with the same degree of professionalism he or she provided prior to the Contractor's request for removal. If the Key Project Staff fails to do so, or if the Contractor removes the Key Project Staff without the State Project Manager's consent, the State has the right to terminate as indicated in D.6 or assess liquidated damages as described in *Pro Forma* Contract Section A.30. - Performance Standards and Liquidated Damages. (Liquidated Damages).

b. <u>Contractor Core Team.</u>

The Contractor shall be responsible for and agrees to provide staff sufficient to complete the Project according to the Master Project Work Plan. In accordance with the Contractor's proposal, the Contractor shall submit a complete listing of the individuals on the Core Project team documenting their corresponding role(s) and an organizational structure diagram of the Project team. The initial Core Team and any subsequent substitution of Core Team members shall require approval by the State. Failure of the Contractor to provide a replacement with equal or greater qualifications within a reasonable time, not exceeding 30 days, may result in Contract termination. The Contractor shall be permitted to add or remove core team positions during the Post-Implementation Support Phase, as approved by the State.

c. <u>Project Team Stability.</u>

The Contractor understands that Contractor's staff turnover is detrimental to Project progress, the quality of the Deliverables and Services to be provided hereunder, and the skills transfer process. The State believes, therefore, that it is in its best interest to maintain the continuity of work assignments for all levels of Employees including, but not limited to the Key Project Staff. The State also recognizes that it can be difficult, or in some cases impractical to maintain said continuity. The Contractor agrees, therefore to make a good faith effort to minimize turnover of Employees it assigns to the Project. The Contractor further agrees that if the Contractor removes an employee who is Key Project Staff prior to completion of his or

her assignment, the Contractor will so notify the State's Project Manager, in writing, five (5) Business Days prior to said Employee's leave date. The Contractor will provide a replacement with similar or better qualifications. The Contractor will ensure that there is a smooth transition, including having the Employee who is leaving train the replacement Employee at the State's facilities.

Cessation of Work by Employees for Reasons beyond Contractor control:

1. Reasons beyond the control of the Contractor shall be defined as: (i) death of the Employee; (ii) new disability or illness; (iii) Employee resigns his or her position; (iv) termination for cause by the Contractor; or (v) any other reasons deemed acceptable by the State's Project Manager.

2. In the event that any Employee ceases work for the reasons specified in A.8.c.1, written notification must be forwarded to the State's Project Manager.

Staff Transition Period

In the event the Contractor initiates a staffing change identified as key personnel under this Contract or who has been onsite full time for a period of six (6) months or greater, and received the State Project Manger's approval as described herein, the Contractor will offer the State a mutually agreed upon transition period up to two (2) weeks. In such event the Contractor, at no cost to the State, shall furnish the State with the service of another Employee possessing the skills required for performance of the Service that would otherwise have been performed by the Employee seeking to replace. Replacement staff must have comparable or greater documented skills than the documented skills of the staff member being replaced. During the transition the departing staff and the new staff will work together to develop a transition plan to transition the responsibilities. The State reserves the right to approve this transition plan in writing.

Work Site and Schedule

The Contractor's team members who have been defined as full-time (100% of working time) within the Master Project Schedule (Contractors' Team), shall perform their duties on-site in Nashville, Tennessee, unless otherwise agreed to by the State in writing. Non full time Contractor staff is not required to be based in Nashville, TN, but shall be available to be on site during their active periods of project engagement, as reasonably requested by the State Project Manager. All team members working onsite shall be identified to the State, along with any Contractor issued equipment intended to be used on site.

The Contractor shall provide State with an advance monthly staff schedule no later than five (5) business days before the last day of the preceding month. Unless otherwise agreed to by both Parties, the Contractor Team will work a schedule on and off site as defined by the State's normal business hours. However, the State of TN holiday schedule and State employees work hours shall be considered for interdependent project tasks and assignments.

A.9. <u>State Provisions.</u>

The State shall provide workspace and internet access for each full-time Contractor personnel working at the project site.

A.10. <u>Deliverable Acceptance.</u>

Deliverables must meet all applicable State approved Acceptance Criteria developed in accordance with State Approved Acceptance Management Plans and Test Plans.

a. <u>Document Based Deliverables.</u>

For each document-based Deliverable other than status reports, the State shall have an acceptance period beginning on the date written Notification of completion was received from the Contractor and as outlined herein. All document-based Deliverables shall require the

written approval by the State Project Manager or his or her written designee that such Deliverables comply with the terms of the Contract.

The Contractor shall provide document-based Deliverables in the form and format agreed to by the State using deliverable specifications sheets approved by the Project Manager. The deliverable specification sheets will include, but not limited to the following information: Deliverable title, frequency, draft and final due dates, approval requirements, outline of contents, and delivery media. See Sample Contract Appendix 10 (Deliverable Specification Sheet).

1. The number of business days for any State initial review of a document-based Deliverable shall be no more than ten (10) Business Days, unless otherwise mutually agreed to in writing by the State Project Manager and the Contractors Project Manager in the Master Project Work Plan. The ten (10) Business Day period shall begin upon written transmittal by the Contractors Project Manager to the State Project Manager that the Deliverable is in final form and ready for approval, and shall be counted from and include the first Business Day following the delivery of the Deliverable to the State. The State shall provide the Contractor (a) with approval of the Deliverable or (b) with a written statement of the itemized deficiencies preventing approval.

2. The Contractor shall have ten (10) Business Days to complete all corrective actions or changes in order for such document-based Deliverable to conform in all material respects with the requirements set forth in the contract. The count of such Business Days shall begin on the first business Day following Contractor's receipt of the written statement of required corrective actions or changes.

3. If the State cannot approve the document based Deliverable after correction by Contractor, the Contractor's Project Manager and the State Project Manager may mutually agree to further steps to correct outstanding material deficiencies. However, in no event shall the total time allocated for review, correction and review of material deficiencies in a Deliverable, exceed thirty (30) business days.

4. The State will have final approval of all document-based Deliverables.

b. <u>Event Deliverables.</u>
For Event Deliverables the State's review process will include an acceptance process as detailed in the approved Acceptance Test Plan. The number of Business Days for any State initial review of an Event Deliverable shall be set forth in the Acceptance Test Plan. If there are multiple events that are part of a single Deliverable, the review process will take place after the final event. The State will determine whether the Deliverable conforms with the requirements set forth in the contract or documented prior to the event in the Acceptance Management Plan, and will approve or prescribe remedy actions for the Contractor consistent with that plan.

c. <u>Other Deliverables.</u>
For Deliverables that contain hardware or software programs, the State's Deliverable review process will include acceptance testing as detailed in an approved Acceptance Test Plan. The number of Business Days for any State initial review/test of a software-based Deliverable shall be set forth in the Acceptance Test Plan. The process for software Deliverables will be as follows. User Acceptance testing will take place in a test environment. After approval by the State, the software Deliverable will be migrated to the production environment. The software Deliverable will then be monitored according to the Production Verification process as described in Contract Appendix 6 (Contractor Requirements) – Table 8. The State will provide Deliverable Acceptance upon completion of Production Verification; the review period will reset starting on the date the State is notified that the correction has been made in the

production system. The State will have final approval of all hardware and software based Deliverables.

A.11. Change Orders.

The State may, at its' sole discretion and with written notice to the Contractor, request changes in the Scope that are necessary but were inadvertently unspecified in this Contract.

a. Change Order Creation.

After receipt of a written request for additional services from the State, the Contractor shall respond to the State, within a maximum of ten (10) business days, with a written proposal for completing the service. Contractor's proposal must specify:

1. the effect, if any, of implementing the requested change(s) on all other services required under this Contract;

2. the specific effort involved in completing the change(s);

3. the expected schedule for completing the change(s);

4. the maximum number of person hours required for the change(s); and

5. the maximum cost for the change(s) — this maximum cost shall in no instance exceed the product of the person hours required multiplied by the appropriate payment rate proposed for such work.

The Contractor shall not perform any additional service until the State has approved the proposal. If approved, the State will sign the proposal, and it shall constitute a Change Order between the Contract Parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this Contract.

b. Change Order Performance.

Subsequent to creation of a Change Order, the Contractor shall complete the required services. The State will be the sole judge of the acceptable completion of work and, upon such determination, shall provide the Contractor written approval.

c. Change Order Remuneration.

The State will remunerate the Contractor only for acceptable work. All acceptable work performed pursuant to an approved Change Order, without a formal amendment of this Contract, shall be remunerated in accordance with and further limited by Contract Section C.3.c., PROVIDED THAT, the State shall be liable to the Contractor only for the cost of the actual goods or services provided to complete the necessary work, not to exceed the maximum cost for the change detailed in the Change Order. In no instance shall the State be liable to the Contractor for any amount exceeding the maximum cost specified by the Change Order authorizing the goods or services. Upon State approval of the work, the Contractor shall invoice the State in accordance with the relevant provisions of this Contract.

A.12. Correction of Deficiencies.

Any corrections of deficiencies relating to the Contract Scope of Services requirements or deliverables and any investigation necessary to determine the source of such deficiencies shall be completed by the Contractor at no cost to the State.

A.13. Inspection and Acceptance.

The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or

performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

A.14. Workflow Business Rule Management.

The statutes, rules and regulations governing State licensing activities change frequently. A primary value proposition of this project is that as laws change and as agencies improve their licensing business processes, the System will enable these changes to be made quickly and easily by business process owners, not software developers. To achieve this objective, the System should be driven by a workflow engine, commonly called a Business Rules Management System (BRMS).

This system core should provide business rules authoring tool set to design, modify, test, deploy, and execute business rules separate from the application code. It should include a rules repository capable of tracking and reverting to older rule versions and tracking changes to rules based on the system user.

The system must provide the capability to guide a business process owner through the definition and creation of license workflows through a graphical user interface.

A.15. Reporting.

The System must generate a variety of reports that are based on the user, audience, and purpose of the report. Requirements range from standard formatted reports used on a routine basis to ad-hoc requests for specific information that is user defined. There will be a great need for a variety of ad-hoc and on-demand reporting of data. Among other things the solution must provide a foundation to standardize processes and information thus enabling management to make much more informed decisions. The success of the project in meeting this objective is tied to the ability for users to access and analyze this information through standard reporting tools.

The vision for reporting is to provide accurate, timely and relevant information to a broad base of information consumers; In this regard, access to licensing information (from the main data store) is essential. In addition, the data will serve as a platform to satisfy a broader scope of strategic informational needs. The reporting environment will be able to:

1. Provide a detailed level of statewide information that does not exist today;
2. Aggregate statewide Information and expand the ability to perform ad hoc queries;
3. Improve the data and methods available to the State staff; and
4. Provide this in an efficient manner, without negatively impacting the transaction processing environment.

It is expected that functionality available through the reporting environment will be enhanced over time and will likely evolve through stages that incrementally provide:

a. The proposed solution must enable the creation and management of the data reporting environment. This should include tools for:
(1). Extracting data from multiple operational databases and external sources;
(2). Cleansing, transforming and integrating this data; and
(3). Periodically refreshing the data to reflect updates at the sources if housed in other than the original sources.

b. Analysis and reporting is the ultimate goal of the reporting solution therefore the proposed solution must provide a robust easy to use set of front end tools to accomplish that goal. Basic elements of the front end toolset include:
(1). The ability to quickly construct both tabular and graphical ad-hoc reports.
(2). The ability to save and share reports with other users and groups.
(3). A choice of delivery methods and automatic scheduling options.
(4). A collection of predefined and customizable report templates and style sheets.
(5). Integration with standard desktop software and third-party reporting software; and
(6). Support for incremental enhancements to delivered functionality.

A.16. Organizational Change Management (OCM).

With the State transitioning from multiple internal and manual systems to new technology and business processes, job roles and organizational structures may be impacted. The Project's OCM resources should collaborate with the Agency's HR representative to determine the impact of these changes on the organization structure and job roles in the State.

This OCM collaboration should also focus on reducing resistance and increasing speedy adoption and productivity during and after the implementation of the future state. This should include, at minimum, an end user Communication Plan, a Training Plan and a comprehensive Change Initiatives Plan. The expected outcome of the OCM Strategy is to reach ultimate productivity and business results as quickly as possible.

A.17. Training Requirements.

The TDA will be a complex system that will be used daily by State staff. The State considers the training of these users to be critical for acceptance of the System as well as the daily use of the System. The System project team will review and approve all Contractor System training staff and user training materials, including training plans and role-based training materials.

The TDA project team training responsibilities include:

a. Review and approval of all role-based System training schedules.
b. Review and approval of all Contractor training staff.
c. Review and approval of the overall System training plan.
d. Identify all staff to be trained during the implementation by role.
e. Review and approval of all Contractor-developed role-based System training materials.
f. Provide training facilities, computers, and network connections for all of the System training sessions.
g. Designate a training environment for use during training.
h. Coordinate training activities with the State's Enterprise Learning Management System as appropriate.

The Contractor will train all applicable State staff and also provide State a "Train-the-Trainer" approach that will allow key State staff to acquire the knowledge of the System necessary to be able to deliver End-user Training. Additionally, the Contractor shall provide technical training for staff who will take over the administration of the System once in production.

A.18. Retainage Period.

The retainage period shall be six (6) months (see item C.3 (b)), shall apply to the entire System and to products or services resulting from change orders and enhancements to the System, and shall begin on the following dates:

(1) The retainage period on the entire System begins with the date the Contractor completes the requirements of Implementation Stage 5 as set forth in RFQ *Pro Forma* Contract Appendix 6, Table 8, System Implementation Phase Requirements certifying full functionality of the System for the last Stage 5.

(2) If any change orders or enhancements are requested by the State subsequent to the implementation stage, the retainage begins on the date the State requesting the change order or enhancement provides written acceptance of the product or services resulting from a change order.

A.19. System Performance and Availability.

a. Following a statewide implementation, the System shall be available continuously, as measured over the course of each calendar month period, an average of 99.9% of the time, excluding unavailability as the result of Exceptions as defined below (the "Availability Percentage"). "Available" means that the System shall be available for access and use by

the State. For purposes of calculating the Availability Percentage, the following are "Exceptions" to the service level requirement, and the System shall not be considered un-Available if any inaccessibility is due to: (i) regularly scheduled downtime (which shall occur only upon advance written notice during non-core business hours); or (ii) loss of the State's Internet connectivity.

Core business hours are defined as:

• 8:00 a.m. – 5:00 p.m. (CT) Mondays through Fridays, excluding State holidays.

Non-core business hours are defined as:
• 5:01 p.m. (CT) Friday – 7:59 a.m. (CT) Monday;
• 5:01 p.m. – 7:59 a.m. (CT) Monday through Friday evenings and selected State holidays;

Core business hours can be changed by the State. Scheduled downtime must be approved in writing in advance by the State.

b. System availability shall be provided at 99.9% availability in any given month, excluding times when the System is un-available as the result of an Exception (as set forth above).

c. The average System response time shall be no more than seven (7) to ten (10) seconds or less for online and web applications. Hourly intervals of monitoring shall be the expected measure. The response time measurement will be the amount of time from the application receiving a request until the user receives the result, i.e., internal application response time between receipt of a request and the requested page being downloaded to the user. The response time measurement shall not include the time required to transmit the user's request to the System.

d. Contractor must immediately notify the State if a standard SLA misses or is outside of variance. Notification must happen through telephone and/or email to customer-provided contacts and acknowledgment of the notification must be logged. The notification should be specific and detailed.

A.20. <u>Acceptable Use Policy and Acceptable Use Agreement.</u>
Contractor personnel who require a physical and/or logical presence (remote connection) within the State of Tennessee networked and/or physical environment must:

a. Ensure that all Contractor personnel maintain an awareness of and remain subject to the State of Tennessee Acceptable Use Policy. Contractor acceptance will be evidenced by the execution of agreements defined in the State's Acceptable Use Policy and User Agreement Acknowledgement. See Contract Appendix 7 for the State's Acceptable Use Policy and Acceptable Use Agreement.

b. A copy of the Tennessee Information Resources Architecture is identified in the State of Tennessee Enterprise Architecture document and will be provided upon request.

A.21. <u>Change Management & Go Live.</u>
The Contractor shall provide the following change management and go-live services:

a. The Contractor shall work with the State to develop change management and Go-Live strategies. These strategies should address but are not limited to the following:

1. Assessing the training needs of the user community.
2. Identifying the most effective format for training delivery.

3. Developing training deliverables.
4. Marketing the system and promoting user adoption.
5. Developing system documentation.

b. The Contractor shall work with the State to assess user training needs and develop training materials. Training materials should be sensitive to user roles (agency analyst, coordinator, executive), cover all system functionality, and be provided in an effective format. One format we would like to explore is screen capture video with voice over, and embedding such videos directly into the system for easy reference.

c. The Contractor shall work with the State to develop detailed system documentation. System documentation differs from training materials in that it defines the system architecture, explains project implementation activities, and demonstrates how the system can be tailored over time to fit evolving TDA needs.

d. The Contractor shall work with the State to and develop a change management implementation plan that culminates in system roll-out.

e. The Contractor shall work with the State to support Go-Live. This support task will be complete when system stability is achieved.

A.22. <u>Help Desk Support.</u>

The following section outlines the State's post Go Live help desk support requirements for the proposed system. The statements in this section are based on the proposed system "as delivered," meaning all software, configurations, and customizations delivered by the contractor during implementation. The contractor will provide the following help desk services after the system Go Live date. These services will be available to the system administrator(s) within:

a. The State prefers the following communication methods:

1. Phone (toll free for the State).
2. Email.
3. Remote System Access – Contractor ability to remotely login to the primary system interface to test functionality and collaborate inquiries.
4. Remote Server Console – The ability to remotely connect to sub-system server console(s) to troubleshoot and resolve issues.

b. Help desk staff will possess intimate knowledge of the delivered system and be capable of troubleshooting complex system issues to resolution. Staff must also be able to provide answers to complex questions. Staff skillset should be equivalent to help desk Tier 3 technical support.

c. Help desk calls will follow the procedure outlined below:

1. Call will be answered by Help Desk staff during hours outlined in A.67.
2. Help Desk staff will remotely connect to the proposed system to verify the issue described by the State.
3. A collaborative discussion will occur between the State and help desk staff to decide the nature of the call and assign call priority.
4. An email will be sent by the help desk to the State confirming the logged call details.
5. The identified issue will be resolved by the help desk within the time allotted by the table below.

A.23. <u>User Licensing.</u>

a. Contractor shall grants the State a perpetual, non-exclusive, transferable license for a

minimum of 250 authorized users to all software necessary to access, run and use the system.

b. Contractor shall allow the State to increase the number of perpetual, non-exclusive, transferable licenses in increments of 10 for all software necessary to access, run and use the system.

c. By entering into this Contract, Contractor waives all terms and conditions contained in its order acknowledgement form, click or shrink wrap agreements, or other contracts or terms and conditions applicable to the Proposed Software which are different from or additional to the terms and conditions set forth in this Contract, and all such different or additional contracts or terms and conditions shall be null and void. The State's acceptance of any licenses granted by Contractor hereunder are expressly made conditioned on the parties' assent to the terms and conditions set forth in this Contract, and is limited to only a license for use of the Evaluated Software. Nothing in this Contract shall bind either party to accept any terms and conditions contained in this Contract for any subsequent contract or enter into a subsequent contract.

A.24. <u>Architecture Management Plan</u>.

The Contractor shall prepare and submit an Architecture Management Plan and shall keep the Architecture Management Plan current to reflect changes and current information. The Architecture Management Plan shall include all known tasks for managing and tracking the architecture activities for the duration of the Project, including the following:

a. A description of how quality attribute scenarios that are included in the *Pro Forma* Contract, Attachment H, will be integrated into the requirements baseline and managed from that point forward.

b. A description of how the technical management approach for ensuring that the System and software architecture descriptions are maintained as enduring "living documents" and accurately reflect all the approved System and software changes that have been subsequently approved and/or implemented since the architecture description was first placed under configuration management control.

c. A description of how the technical approach for implementing architecture compliance reviews required to be periodically conducted throughout the System life cycle, under State oversight. The objective of conducting these architecture compliance reviews (after the iterative design reviews have been completed) is to verify that the detailed design and software implementation complies with the approved System and software architecture baseline that is under configuration management control. As part of the approach, the Plan shall include a description of how often and when such architecture compliance reviews should be conducted to achieve the stated objective.

d. A description of the information the Contractor is going to collect, and report on, to track and manage all the architecture-related tasks described above.

A.25. <u>Conduct Project Kick-off Meeting.</u>

The Contractor shall conduct a Project "Kick-Off" Meeting with representatives of TDA to commence the Project. This meeting shall focus specifically on the responsibilities of the Contractor and working relationships and interactions among the Contractor and State staff, as set forth herein and shall include a review of the Master Project Work Plan. Presentation materials and handouts shall be developed by the Contractor and presented for review and approval, prior to the Project Kick-off Meeting. The Contractor shall provide attendees a written summary of the meeting immediately thereafter.

A.26. <u>Project Steering Committee (PSC).</u>

The PSC provides executive level guidance for the I Project. The PSC shall evaluate the Project at critical review points as defined by the State during the entire life cycle of the Project. The evaluation shall consider information from Project management and technical groups supporting the Project such as database administration, technical systems support, and computer operations.

A.27. Narrative Project Status Report and PSC Presentation.

At a minimum, the Contractor shall make a semi-monthly presentation to the PSC. The narrative Project Status Report and presentation shall be provided that details the progress of the Project, identifies the monthly activities of the Project, documents upcoming key activities and identifies the issues and items needing PSC attention. The PSC may request unscheduled reports from the Contractor to address specific concerns relating to the Project status.

A.28. Intentionally left blank

A.29. Intentionally left blank

A.30. Performance Standards and Liquidated Damages.

The Contractor shall comply with minimum system and procedural performance requirements. At the first incident of failure to meet one or more of the defined performance standards, the State, in its independent discretion, may request a corrective action plan and establish an extension date by which the Contractor shall correct the deficiency. Continued failure to meet performance standards may result in imposition of the damages established in this paragraph or in the State deeming the Contract to be in breach.

The following table defines the standards required for Contractor performance for the Project and the associated liquidated damages, which the Contractor agrees to pay. The Contractor agrees that the amounts set forth in the table below represent a reasonable estimate of the damages that would occur from a breach, and that, due to the nature of the Contractor's obligations under this Contract, such amounts would be uncertain and not easily proven.

Performance Area	Performance Item	Performance Period	Liquidated and Additional Damages
Response time	The Project performance thresholds for application System response time as required by Section A.19.		One Thousand Dollars ($1,000.00) per day
Availability	The Project performance thresholds for application System availability as required by Section A.19.		Ten Thousand Dollars ($10,000.00) per day
Applications, Permits, and Renewals	Failure to issue TDA timely and accurate applications and permits which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from applicable go-live date.	$7,500 per day
	Failure to issue timely and accurate Renewal Notices for TDA licenses on the predetermined dates based on expiration period in which failure is solely due to the fault of the Contractor software, system	6 months from applicable go-live date.	$7,500 per day

Performance Area	Performance Item	Performance Period	Liquidated and Additional Damages
	configuration, or due to Contractor action.		
Bill and Fee Collection	Failure to accurately account for all monies assessed and collected through the Contractor system, which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from applicable go-live date.	$5,000 per day
	Failure to accurately and timely integrate with iNovah cashiering system, period in which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from applicable go-live date.	$5,000 per day
	Failure to accurately generate a single consolidated invoice per Entity for all TDA assessed fees in which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date	$1,000 per day
Inspections	Failure to accurately capture inspection data and/or sample information on supported portable devices in a non-connected environment, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$1,000 per day
	Failure to generate accurate and timely Notices, Violations, and Inspection Reports, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$1,000 per day
	Failure to capture and associate uploaded attachments to inspection records, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$1,000 per day
On-Line Services	Failure to provide a secure user interface to which the Public may apply for and pay for multiple TDA Licenses via the internet,	60 days from the applicable go-live date.	$2,000 per day

Performance Area	Performance Item	Performance Period	Liquidated and Additional Damages
	which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.		
	Failure to accurately and timely interface with the State Authorized Payment Card Vendor, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$2,000 per day
System Performance	In a Severity Level 1 event as defined in A.67 Support, failure of the contractor to resolve the issue within the agreed upon service level agreement, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	30 days from the applicable go-live date	$2,000 per hour
	In a Severity Level 2 event as defined in A.67 Support, failure of the contractor to resolve the issue within the agreed upon service level agreement, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	30 days from the applicable go-live date	$1,000 per hour

A.31. Right to Remove Individuals.

The State shall have the right at any time to require that the Contractor remove from interaction with State any Contractor representative who the State believes is detrimental to its working relationship with the service provider. The State shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the contract or future work orders without the State's consent.

A.32. Subcontractor Disclosure.

The Contractor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.

A.33. General.

The Contractor shall provide a Customized Solution - either Commercial Off-The-Shelf (COTS) Software OR Software Programs developed by the Contractor plus any other services or deliverables as required, described, and detailed herein that shall meet all service and delivery timelines as specified by this Contract. The solution must be housed in one or more of the Contractor's secure Data Centers or by a third party at one or more remote secure Data Centers that meet the requirements of this contract. The solution can be a cloud hosted SaaS (Software

as a Service) solution. The State defines cloud hosted SaaS solution as an application offered to a user as a service. SaaS is a complete, turnkey application solution (that is, no IT organization-built solution is required). User access must be via a user-centric interface, such as a Web browser. The Contractor shall use Web Services exclusively to interface with the State's data in near real time when possible.

A.34. Legal Compliance.

All System security shall be compliant with TN Enterprise Information Security Policies. The security policy is included in *Pro Forma* Contract Appendix 9 – Enterprise Information Security Policies.

Transmission/dissemination of all data must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."

The Contractor shall be compliant with PCI DSS v3, PCI PA-DSS v3, or other regulations that are relevant to this contract.

The Contractor will be responsible for review of existing Federal and State legislation, as well as guidance and other program or technical documentation. In addition the Contractor shall be responsible for review of existing documentation generated, maintained, or provided by the State, including initial requirements, process flows, policies, or other documentation. The Contractor shall be responsible for review of the State's current processes and system design. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

A.35. Reporting and Continuous Monitoring.

The contractor shall maintain a security management continuous monitoring environment that meets or exceeds the requirements in the Reporting and Continuous Monitoring, based upon the latest edition of SOC2 Type II, SOC3, or ISO27001 Cloud Computing Security Requirements Baseline and Continuous Monitoring Requirements. To safeguard against threats and hazards to the security, integrity, and confidentiality of any State data collected and stored by the Contractor, the Contractor shall afford the State access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the State as required by SOC2 Type II, SOC3, or ISO27001 security standards.

A.36. Miscellaneous Security Provisions.

The Contractor shall prepare and deliver a comprehensive written Security Plan describing how the System's application security features shall satisfy the security requirements found in this contract. The Plan shall include all recommended levels of security, limitations of capabilities, and any required rules, and shall incorporate any reasonable and lawful requests or requirements of the State. The format and content of security tables shall be included, as well as the recommended starting phase for establishing security profiles. Further, and without limitation, the Security Plan shall demonstrate how Contractor shall:

1. Protect all information and information systems in order to ensure:
    a. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information authenticity;
    b. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
    c. Availability, which means ensuring timely and reliable access to and use of information.

2. Secure the System and the information contained therein that connects to the State network, or any network operated by the Contractor, regardless of location.

3. Adopt and implement, at a minimum, the policies, procedures, controls, and standards of the States' Information Security Policies to ensure the integrity, confidentiality, and availability of information and information systems for which the Contractor is responsible under this contract or to which it may otherwise have access under this contract.

4. Conduct periodic and special vulnerability scans, and install software/hardware patches and upgrades to protect all automated information assets. These audits shall be performed by a third party qualified to perform such tests, including penetration tests of the internal and external user interface, annually. The Contractor must submit, for review and approval by the State, the proposed scope of testing as well as the name and qualifications of the party performing the tests. The Contractor is responsible for the costs of this testing. The State may elect to perform independent testing. The Contractor must address and resolve any application vulnerabilities as directed by the State. The Contractor must arrange for repeat testing to ensure that all identified vulnerabilities have been addressed as directed by the State.

5. Report the results of the scans described in no. 4, above, to the State on a monthly basis, with reports due 10 calendar days following the end of each reporting period.

The Contractor shall ensure that each user's role is based on the business functions they are required to perform. The State has the right to perform manual or automated audits, scans, reviews, or other inspections of the Contractor's IT environment being used to provide or facilitate services for the State. The State reserves the right to verify the infrastructure and security test results.

The Contractor shall not publish or disclose in any manner, without the State's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the State.

Access to State Data shall be limited to the Contractor's State-assigned employees. Staff with data access shall sign a nondisclosure agreement and a security agreement. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of State data, the Contractor shall afford the State access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

The Contractor shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Contractor. The State and the Contractor shall understand each other's roles and responsibilities.

The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own personal data.

Contractor must secure and encrypt all APIs and Open Interfaces.

No click through licenses or provisions will be allowed.

A.37. <u>Physical Security.</u>

All enterprise data processing facilities that process or store data shall have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference. Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel. Procedures for working in secure areas should be created and implemented. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities. Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Secured cabinets or facilities should support further segregation based on role and responsibility.

Users should ensure that unattended data processing equipment has appropriate protection. All systems and devices owned and operated by or on behalf of the State should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The Contractor may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

A.38. <u>Assessment of the System.</u>

1. The contractor shall comply with requirements, including making available any documentation, physical access, and logical access needed to support this requirement. The contractor shall create, maintain and update logs and documentation according to certification standard controls.

2. Information systems must be reassessed by the State whenever there is a significant change to the system's security posture.

3. The State reserves the right to perform Penetration Testing. If the State exercises this right, the Contractor shall allow State employees (or designated third parties) to conduct Security Assessment activities to include control reviews. Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of State information for vulnerabilities.

4. The Contractor is responsible for mitigating all security risks found during Assessment and continuous monitoring activities. All high-risk vulnerabilities and moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The State will determine the risk rating of vulnerabilities.

The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the Standard State Desktop Configuration. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved configuration. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. Contractor shall provide all services requested through this Contract within the context of the technical environment described in *Tennessee Information Resources Architecture*.

A.39. <u>Protection of Information.</u>

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their own proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as

applicable to Privacy Act Information. The State will retain unrestricted rights to State data. The State also maintains the right to request full copies of the data at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as Personally Identifiable Information (PII). This data shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure. The data must be available to the State upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the State..

A.40. Confidentiality and Non-Disclosure.

The State has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the State and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the State during and at the end of this contract. The contractor shall not release any information without the written consent of the State. Personnel working on any of the described tasks may, at State request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of State information and documents. Data will only be disclosed to authorized personnel on a Need-To-Know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. Any information made available to the Contractor by the State shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of State records. Each officer or employee of the Contractor to whom any State record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions.

A.41. Data Ownership.

The State will own all right, title and interest in its data that is related to the services provided by this contract. The Contractor shall not access State user accounts or State data except:

1. In the course of data center operations,
2. In response to service or technical issues,
3. As required by the express terms of this contract, or
4. At the State's written request.

All data obtained by the Contractor in the performance of this contract shall become and remain the property of the State.

Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of State information and comply with the following conditions:

1. At no time shall any data or processes that either belong to or are intended for the use of the State or its officers, agents or employees, be copied, disclosed or retained by the Contractor for subsequent use in any transaction that does not include the State.
2. The Contractor shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

A.42. Data Location.

The Contractor shall provide its services to the State and its end users solely from data centers in the United States of America. Storage of State data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access State data remotely only as required to provide technical support solely within the U.S.

A.43. Encryption.

All data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the data. The Contractor shall ensure drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data. The solution should support 256 bit encryption or latest State standard. This provision also applies to the data-at-rest and data-in-transit protections provided by the solution, even if protection of data-at-rest and/or data-in-transit is implemented by external modules (rather than the solution itself). The State will hold all encryption keys.

A.44. Import and Export of Data.

The State shall have the ability to Import or export data piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the State to import or export data to or from other service providers.

A.45. Data Protection.

The Contractor represents and warrants that use of the System as contemplated hereunder including, without limitation, Work Product and any software, will not result in the loss, destruction, deletion or of data integrity issues of any State's data that is not easily retrievable or the alteration of any of State's data that is not easily reversed.

A.46. Payment Card Industry Data Security Standard (PCI DSS).

Payment Card Industry Data Security Standard (PCI DSS) v3 and PCI _PA-DSS v3) compliance is mandatory. Proof must be through an annual audit by a Qualified Security Assessor (a designation received from the Payment Card Industry Security Standards. (https://www.pcisecuritystandards.org/security standards)

A.47. Separation of Duties.

To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities.

Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible. The Contractor shall limit staff knowledge of State data to that which is absolutely necessary to perform job duties.

A.48. Security Incident and Data Breach.

The Contractor shall inform the State of any security incident or data breach. The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the State should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

The Contractor shall report any security incident to the appropriate State identified contact immediately. If the Contractor has actual knowledge of a confirmed data breach that affects the

security of any State content that is subject to applicable data breach notification law, the Contractor shall

1. Promptly notify the appropriate State identified contact within 24 hours or sooner, unless shorter time is required by applicable law,
2. Take commercially reasonable measures to report perceived security incidents to address the data breach in a timely manner
3. Cooperate with the State as reasonably requested by the State to investigate and resolve the data breach,
4. Promptly implement necessary remedial measures, if necessary, and
5. Document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

Unless otherwise stipulated, if a data breach is a direct result of the Contractor breach of its contract obligation to encrypt personal data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law - all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

A.49. <u>Access to Security Logs and Reports.</u>

The Contractor shall provide reports to the State in a format as agreed to by both the Contractor and the State. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this contract.

A.50. <u>User Registration, De-Registration, Provisioning and Access.</u>

User access to information resources should be authorized and provisioned according to the Agency's employee provisioning process. Users should have the least privileges required to perform their roles as identified and approved by their agency. The allocation and use of privileged access rights should be restricted and controlled. A user's access rights should be reviewed validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies). All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day. All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in State managed data processing facilities or facilities operated on behalf of the State must use a multifactor VPN solution to obtain access.

Contractor must provide a Web interface in which an administrator can create, manage and delete user accounts. This interface will create sub-administrator accounts and configure IAM services. The Web interface must be supported for use in all major Web browsers. Contractor must support Security Assertion Markup Language (SAML).

The solution should support the ability to display the State Acceptable Use Policy (AUP) statement after unlocking the container on the device and ability to confirm acceptance.

A.51. <u>Removable Media.</u>

Removable media should be sanitized prior to removing it from the facilities for maintenance or repair. Removable media should be disposed of securely when no longer required, using approved State procedures. Removable media containing confidential information, confidential

data, or sensitive data must be protected against unauthorized access, misuse or corruption during transport.

A.52. Change Control and Advance Notice.

The Contractor shall give advance notice to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

A.53. Security Certification, Accreditation, Audit.

At the State's request, the contractor shall provide proof of certification, accreditation, or audit on a yearly basis to the State to validate the hosting solution security. (Examples: SOC 2 Type II/ SOC 3, ISO 27001).

A.54. Malicious Code.

The Contractor shall represent and warrant that the Software, Application and Network shall be free from all computer viruses, worms, time-outs, other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the Software user's or another's software, hardware, networks, data or information. If the Contractor is aware of any security incident, vulnerability or other malicious code within their software or network the Contractor shall immediately disclose this information to the State via telephone and e-mail, as well as identify a timeline to mitigate and eliminate the risk.

A.55. System Interfaces.

The Contractor is required to exchange information between the State System and entities that are internal or external to the State. The discovery phase of the design process must include evaluation of the existing interfaces and specify modifications, enhancements, or replacements to the interfaces which must be integrated into the system. The Contractor shall develop interfaces that feature standardized data formats and characteristics as well as standardized methods of communication and data interchange where applicable. The Contractor must also provide data schema and mappings and a fully documented set of standard application interfaces to allow for future external data sharing.

The Contractor shall develop specification documentation for each interface incorporated into the State system during the Design Phase of this project. The Interface Specifications shall be non-proprietary and the property of the State. The State shall have full distribution rights to the interface specifications developed for the system. The system shall provide State staff the ability to select the method of interchange. Interfaces may be real time, batch or a combination of both.

RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common contains a list of known system interfaces but does not constitute a comprehensive list of all needed interfaces that will be necessary for successful implementation. Some interfaces require encryption. The Contractor shall use encryption for data transfers. Protocols associated with specific interfaces shall be determined by the Contractor and approved by the State during design.

The Contractor must be able to integrate with the State’s provider of Credit Card and Check Processing.

A.56. Content and Document Management Capability.

The System must incorporate content management capabilities. Content management is needed to manage and automate the publishing of licensing-related content via workflows. The System must incorporate document management capabilities. State employees and business entities have a need to provide documentation to satisfy licensing requirements. The System must offer

the ability to upload, scan, store, index, archive, and retrieve these documents. A reportable audit trail must exist for each document, including upload, modified, accessed, deleted dates, and retention schedule-related actions.

The State wants the option to integrate their document management system with the System or to make use of document management available within the System.

Users must be able to upload electronic documents to the System as necessary at any point in a license application workflow. The documents must be associated with the applicant's profile, license application or any individual license transaction. Paper documents and forms must be submitted in some licensing processes. The System must accommodate scanning, storage and retrieval of these image files.

The system shall indicate that the required document has been scanned and maintain a link to the scanned image of all documents in the State's document management system. The system shall allow for electronic capture of customer's signature on any required documents.

The system shall allow for the viewing of all scanned documents. The contractor shall develop a Scanning Integration Design and obtain State approval of this design during the design phase of this project. The design shall show in detail how the system will integrate with the State's standard document management system and fulfill all of the requirements stated above. The printing of scanned images shall be limited to authorized state staff.

A.57. <u>System Hardware.</u>

All hardware will be hosted by the Contractor at either one or more of the Contractor's secure Data Centers or by a third party at one or more remote secure Data Centers. Each of these locations should meet the requirements of this contract.

The Contractor is responsible for providing all hardware needed to fulfill the requirements of the contract. The Contractor shall provide clear specifications of all hardware that is needed. The Contractor shall size the hardware to sufficiently meet the business need but not exceed what the State considers a reasonable amount of capacity. The Contractor shall deliver a Hardware Capacity Analysis and Growth Plan showing how the hardware requirements were derived and how to forecast additional hardware needs as system utilization and storage requirements increase. The State reserves the right to add change, reconfigure, consolidate or eliminate hardware at any time to meet the best interests of the State.

The Contractor represents and warrants that the System and specified hardware are fully compatible and interoperable with each other and with all third-party software and hardware products that the Contractor's marketing materials, product documentation, or RFQ references. In addition, Contractor shall provide all services requested through this Contract to be compatible with the technical environment described in the Tennessee Enterprise Technology Architecture Standard Products.

A.58. <u>Environments.</u>

The Contractor shall have four operating environments:

1. *Development* - Used for development of programmatic changes. Must be similar to production environment, but can be smaller in scale. This environment hosts the source code library, versioning/configuration management/release tools, and other software development and testing tools as needed.

2. *System Integration Test* - Used to verify new or modified code integrations with the current application baseline. Must accurately represent the production environment for the changes being tested, but does not require duplication of the entire production data set.

3. *Training* - A small scale mockup of the production environment, capable of representing the current production version or new versions soon to be implemented into production. This environment will be used to train users ongoing with real production data without making changes to the production database.

4. *Production* - The official system of record. In a cloud environment, the production environment shall provide sufficient elasticity to meet expected peaks in demand. Changes to the production environment are made only through documented change control procedures. The production environment shall be physically and logically isolated from the Development, System/Integration Test, and Training environments.

A.59. System Performance Monitoring and Tuning Utilities.

The system shall include all utilities for software performance monitoring and tuning. The Contractor shall be responsible for the performance monitoring and tuning activities of the system. The Contractor must perform regression testing on upgrades prior to installing or implementing the upgrades into production. For any new version or upgrade of the software, the Contractor must certify in writing to the State that all the previous capabilities still work in accordance with the contract requirements.

A.60. Intentionally left blank

A.61. Maintenance.

System Maintenance shall include all services necessary to maintain the system operational uptime and recovery from system failures. The Contractor must be proactively monitoring the system and not relying solely on the State to notify the Contractor of system problems.

The Contractor shall include a calendar of scheduled maintenance, which shall be updated, revised, and coordinated with the State quarterly, with all scheduled activities occurring within the maintenance periods set forth herein. Contractor shall not have more than 30 minutes of scheduled maintenance per month and must provide at least three business days of notice. The Contractor shall provide for infrastructure maintenance, upgrades, and enhancements over time. The Contractor shall include the following Infrastructure Maintenance services including, but not limited to:

1. Maintenance of all tiers from the infrastructure to the application;
2. Continuous performance monitoring;
3. Bug fixes, enhancements, including new features, functionality, and technology upgrades
4. Quality assurance and testing of modifications and upgrades;
5. All patch updates
6. Changes mandated by any state or federal statute or regulation;
7. Increases in data storage or transaction capacity;
8. Backup and restore;
9. Disaster recovery;
10. Sufficient networking bandwidth and hardware capacity to support the peak processing demands of the State;
11. Operational independence of the State; and.
12. Redundancy. The Contractor shall offer a fully redundant solution that will provide full business continuity.

A.62. Maintenance Log.

The Contractor shall keep a log of all maintenance technical support calls made to the help desk, technical maintenance and technical support personnel and document the complaints and problems reported to the help desk system by the State. The log shall be made available to the State as part of an electronic monthly reporting as well as any other time upon request by the State. The log must at a minimum contain the following information:

1. Date and Time of call;
2. Name of Caller;

3. Caller's Organization Name;
4. Caller's telephone number and/or email address;
5. Description of Reported Problem/Complaint;
6. Indication of whether the problem/compliant was resolved at time of call;
7. Description of any follow-up investigation/resolution plans;
8. Assigned Case number and
9. Date, Time and Description of Final Resolution.

A.63. <u>Benchmark Tests.</u>

To determine the growth and reliability of the System, the Contractor shall design and perform benchmark tests. The benchmark shall be designed to produce information that supports projections of system performance characteristics and capacity projections of the System under statewide operations for the contract life following the State's implementation. The benchmark shall also address stress tests at each level of technology employed by the System. A capacity simulation and benchmark report documenting the projections shall be submitted to the State for review and approval.

A.64. <u>Capacity Planning.</u>

The purpose of the Capacity Analysis and Evaluation Plan is to identify users and interfaces of the System and to assist State technical, operations, and telecommunications personnel in projecting the capacity requirements needed (disk space, memory, etc.) and communication requirements (bandwidth, lines, etc.) to support the System. The Contractor shall document the approach for the selection and utilization of computers and services (applications, communications, databases, gateways, firewalling, etc.) that provide a modular, scalable solution that meets the State's minimum performance objectives as defined below. The Contractor shall provide the planning coordination for the network to achieve the minimum performance standards required by the State and shall perform all System modifications required to ensure System performance meets the required performance standards. The Contractor's design and implementation solutions for capacity will be reviewed and evaluated during the Design and Development Phases as by the State. The approved capacity solutions involving hardware will become the minimal environment requirements.

The Contractor shall prepare interim and final Capacity Evaluation Reports which documents, in detail, the results of the tests and recommendations for resolving any problems, as outlined in the Capacity Analysis and Evaluation Plan. The Contractor shall provide detailed documentation demonstrating how the required response time shall be achieved by the application. A basis for all calculations and assumptions are to be shown. At a minimum, the documentation shall show line speeds, devices supported per circuit and per location, routing, average and peak traffic load, and average and worst case response times. The Contractor shall provide to the State all information about the impact of application solutions.

The Contractor shall provide written affirmation and validate that State's production environment shall support the Project in a full production capacity and meet performance standards. The Contractor shall conduct a Capacity Evaluation Test during the Development Phase of the Project that addresses the needs and performance measurements identified in the Capacity Analysis and Evaluation Plan. Capacity Evaluation Testing shall be performed at a system level by the Contractor and in cooperation with the State Project team during the development Phase of the Project. The Capacity Evaluation Test shall include a stringent stress test that includes a simulation of workload and volume testing for the State, which shall be used to test and monitor the limits of the System in a simulated production environment The Capacity Evaluation Test shall be performed at peak times with peak volumes. The Capacity Evaluation Test results shall determine whether the application conforms to acceptable response and hardware load conditions. The Contractor shall be required to perform capacity testing multiple times until satisfactory test results are obtained. The capacity test results shall confirm that the software and the hardware configuration meet the State's requirements.

The Contractor shall perform all application software, file structure, database, and system software modifications necessary to ensure system performance reaches acceptable levels in production environments, based upon the results of the benchmarks or the capacity simulation models. The Contractor shall work with the State's staff to make other modifications necessary to ensure system performance reaches required performance standards in a production environment based on the results of system testing.

A.65. Scalability.
The Contractor represents and warrants that the System has the capacity to scale up to meet the States' processing load without requiring time to add infrastructure. This scaling must include scaling service up or down rapidly in terms of users, storage or network.

A.66. Storage.
Contractor will impose no limit to the State on the amount of storage utilized in the solution provided.

A.67. Support.
When the State staff calls the help desk/technical support, the Contractor's technical support staff should not place the State caller on hold for more than five (5) minutes.

The following table lists the State's Service Level Objectives. These Service Levels should serve as a guideline of the level of response and resources the State is seeking for all of the support periods. The Contractor shall propose Service Levels with these guidelines in mind.

Defect Severity Level 1 - Maximum Response Time Immediately and up to 2 hours after notification. Contractor will provide resources to fix until completed. Coverage will be provided 24 hours per day and 7 days per week. These are defined as urgent situations, when the State's system is down and the State is unable to use the system. A Level 1 Defect may have one or more of the following characteristics: (a) a critical function of the Application/Device is not available; (b) the Application/Device hangs indefinitely and/or causes other State applications to hang; (c) the Application/Device crashes and/or causes other State applications to crash; and/or (d) a security incident has occurred or is suspected to have occurred.

Defect Severity Level 2 - Maximum Response Time Immediately and up to 4 hours after notification. Contractor will provide resources to fix until completed. Coverage will be provided 24 hours per day and 7 days per week. These shall be defined as critical system component(s) that has significant outages and/or failure precluding its successful operation, or possibly endangering the State's environment. A Level 2 Defect may have one or more of the following characteristics: (a) the performance, functionality or usability of one or more of the Application/Device's parts is severely degraded; (b) multiple users are impacted; and/or (c) one or more business functions are unavailable or unusable by the end users. The system may operate, but is severely restricted. Failure causes a loss of function or data, but there is a mutually agreed upon workaround.

Defect Severity Level 3 - Maximum Response Time Immediately and up to 2 business days after notification. Contractor and State will agree to resources applied. Coverage will be provided from 8:00 a.m. to 6:00 p.m. CT weekdays [Excluding State Holidays]. These shall be defined as a failure of a system or part thereof which has a minor impact on a State business process and can be handled on a non-immediate basis. Examples may include user requests (e.g., a report is not formatted correctly) and peripheral problems (e.g., output fails to print properly).

Defect Severity Level 4 - Maximum Response Time as mutually agreed. Contractor and State will agree to resources applied. Coverage will be provided from 8:00 a.m. to 5:00 p.m. CT weekdays [Excluding State Holidays]. These shall be defined as cosmetic and minor errors; all

the user tasks can still be accomplished. Example: Grammar errors, color changes, misspelled words, layout, etc.

The State reserves the right to determine and assign levels of severity for the issue/support problems.

The Contractors' technical support staff shall accept the call for assistance at the time the State places the initial call.

Contractor shall not close a Defect fix unless the fix has been demonstrated to either: (a) repair the functionality, performance and usability of the Application or Device to its pre-Defect level or (b) improve the functionality, performance and usability of the Application or Device from its pre-Defect level. Unless, for a particular defect, the State has provided prior written approval for different response times, the Contractor shall, for each calendar month and for each Severity Level, respond to one hundred percent (100%) of reported Defects within the Maximum Response Time during Hours and Days of Coverage agreed upon for each level of defect.

The State defines the problem resolution response time as the total elapsed time from when the Contractor's Help Desk has been contacted by the State and the system error/nonconformity severity level has been determined until the time when the issue or problem has been fixed, tested, and verified as being resolved as reasonably determined by the State in accordance with the aforementioned severity level provisions.

A.68. <u>Termination or Suspension of Service.</u>

In the event of a termination of the contract, the Contractor shall implement an orderly return of State data in a mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of State data. The State shall be entitled to any post-termination assistance generally made available with respect to the services.

During any period of service suspension or in the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase any State data for a period of 365 days after the effective date of suspension or termination.

After such period, the Contractor shall have no obligation to maintain or provide any State data.

When no longer required, information, data, and/or equipment will be returned to State control, destroyed, or held until otherwise directed at the State's discretion. Destruction of items shall be accomplished by following NIST Special Publication 800-88 or adherence to DoD 5220.22-M, Guidelines for Media Sanitization. Certificates of destruction shall be provided to the State.

A.69. <u>Turnover/Transition Plan</u>

The Contractor shall provide a Turnover/Transition Plan as part of this contract. Turnover is defined as those activities that are required for the Contractor to perform in order to transition contract operations to the State or a subsequent Contractor at the termination of the agreement. During the turnover the Contractor must ensure that program stakeholders do not experience any adverse impact from the transfer of services. The Contractor must fully cooperate with the State in achieving a smooth transition.

The Contractor shall create a Turnover/Transition Plan during the Initiation Phase and shall submit the Plan for approval by the State. The Contractor shall keep this plan current with any changes in subsequent phases. The Contractor shall outline its plan for turnover of the System from Contractor support to the support by the State. The Turnover/Transition Plan shall include the state of readiness required for System turnover, should it be required for transference or migration by the State, and shall outline the conditional criteria required to turn over responsibilities for the operation and support of the System from the Contractor staff to the State and the essential knowledge transfer to the State. The Contractor shall develop detailed

specifications for describing States' staff responsibilities for System operations, support, and maintenance. The Turnover/Transition Plan shall describe all tasks to be performed by the State, and the Contractor to ensure a smooth transfer of services.

A.70. Notification of Legal Requests.
The Contractor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's data under this contract, or which, in any way might reasonably require access to the data of the State. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice.

A.71. Contract Audit.
The Contractor shall allow the state to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

A.72. Intentionally left blank

A.73. Disaster Recovery.
The Contractor will deliver thirty (30) calendar days before the system is implemented and maintain the plan throughout the life of the contract, a Business Continuity and Disaster Recovery (BC-DR) Plan, which is updated and tested at least annually and is subject to approval by the State. The plan must address recovery of business functions, business units, business processes, human resources, and the technology infrastructure.

The plan must ensure that the State's Recovery Point Objectives (RPO) of 24 hours and recovery time objective (RTO) of 48 hours are met. The Contractor shall continually review the Disaster Recovery Plan and make necessary updates to the plan at least annually to ensure the plan always contains accurate and up-to date information.

This plan shall include procedures for the periodic copying of data to other media and the process for restoring data to its original or prior form. The Contractor will be required to provide written evidence of this to the State. This evidence should be in the form of a detailed report describing the date tested, types of systems tested, outcome of tests, and any remedial items that testing may discover. Regardless of the architecture of its systems, the Contractor shall develop and be continually ready to invoke a business continuity and disaster recovery plan. The BC-DR plan shall encompass all information systems supporting this Contract. At a minimum the Contractor's BC-DR plan shall address the following scenarios:

1. Central and/or satellite data processing, telecommunications, print and mailing facilities and functions therein

2. System interruption or failure resulting from network, operating hardware, software, communications infrastructure or operational errors that compromise the integrity of transactions that are active in a live system at the time of the outage;

3. System interruption or failure resulting from network, operating hardware, software, communications infrastructure or operational errors that compromise the integrity of data maintained in a live or archival system; and

4. System interruption or failure resulting from network, operating hardware, software, communications infrastructure or operational errors that do not compromise the integrity of transactions or data maintained in a live or archival system but does prevent access to the system.

The Contractor shall periodically, but no less than annually, test its BC-DR plan through simulated disasters and lower level failures in order to demonstrate to the State that it can restore system functions. The Contractor shall submit an annual BC-DR Results Report to the State.

In the event that the Contractor fails to demonstrate in the tests of its BC-DR plan that it can restore system functions per the standards outlined in this Contract, the Contractor shall submit to the State a corrective action plan that describes how the failure will be resolved. The Contractor shall deliver the corrective action plan within ten (10) business days of the conclusion of the test.

In the event of a declared major failure or disaster, as defined in the Contractor's BC-DR plan, the Contractor's critical functionality, needed to perform the services under this contract, shall be restored within one hour of the failure's or disaster's occurrence. All State data shall remain within the continental United States of America.

The Contractor shall maintain a duplicate set of all records relating to this Program in electronic medium, usable by the State and the Contractor for the purpose of disaster recovery. Such duplicate records are to be stored at a secure fire, flood, and theft- protected facility located at least 25 miles away from the storage location of the originals. The Contractor shall update duplicate records, at a minimum, on a daily basis and shall retain said records for a period of one hundred and eighty (180) days from the date of creation.

A.74. Archiving.

The Contractor shall facilitate implementation of records management policies through a systematic archiving capability to meet requirements for statutory reporting and compliance. Archived information should be retrieved quickly and efficiently without adversely impacting performance and should fulfill public records retention and disposition requirements. Archived data must retain its historical business context.

A.75. Data and System Conversion.

All data in the scope of the required functionality, current and historical, from all existing State systems shall be converted from the existing systems into the new system. The existing license, permit, certification numbers must be maintained in the same size and format as the current license, permit or certification number.

All data being converted shall be “cleaned” prior to conversion, including but not limited to remediation of duplicated data, cleansing addresses and correcting known data errors. The Contractor shall manage the overall data cleansing process. The Contractor shall have sufficient logic in their conversion programs to detect and resolve data inconsistencies which can be resolved programmatically with a high level of confidence. For those data which cannot be reliably converted, the Contractor shall provide a report of those data, and provide a mechanism for recording corrections such that a) data which must be corrected by hand shall only require keying the changes, not the entire data value, and b) corrections shall be done in an orderly process which insures that all hand-correctable data is reviewed and corrected. The Contractor shall define specific data conversion algorithms at the applicable phase of the project for approval by State staff.

During the design phase, the contractor shall develop a Data Conversion Plan and obtain plan approval from the State. The plan shall describe data cleansing and conversion methods, identify the mapping of all data in scope to the new system, including all data transformations needed. The Conversion Plan ensures information integrity and the validity of the electronic content is maintained throughout the conversion and implementation phases. The Contractor shall work with the IT staff of the State to map data fields from each legacy system to the Contractor’s system, in preparation for the data conversion process. The Contractor shall provide data conversion rules for the State. The Contractor shall document data migration requirements and submit these requirements to the State for review and approval.

During the construction phase, the contractor shall develop and test data cleansing and conversion procedures (custom software programs, conversion tool configurations or scripts as needed). The contractor shall provide test results, control totals, record counts, etc., of the data

before and after the conversion, and an audit of data before and after conversion for review and approval by the State.

During the implementation phase, the contractor shall provide data conversion results for State approval prior to implementation. The results shall include samples of converted data, control totals, record counts, etc., of the data before and after the conversion, and an audit of data before and after conversion. During the implementation phase, all data shall be kept synchronized between the existing systems and the State system as necessary to keep implemented locations in synchronization with those not yet implemented. The Contractor shall perform functional, system, and integration testing to ensure all data was successfully converted and the system functions as expected after legacy data has been placed into the system. The Contractor shall correct all problems reported.

The Contractor shall convert electronic content from legacy systems that are being fully or partially replaced within the scope of the Project. The Contractor shall define the electronic content conversion process that will be used for each of these legacy systems. Integration testing shall be performed and results documented on this converted electronic content, prior to User Acceptance Testing. The plan shall address, at a minimum, the following to store its electronic content on the System's Electronic Content Repository:

1. Roles, responsibilities, and required staffing to support conversion.
2. Conversion overview noting objectives, approach, roles, techniques, testing process, electronic content validation, impact, and resources.
3. Conversion strategy for handling "black out" period when switching from the old system to the new and the interfaces associated with each.
4. Conversion process (automated manual, verification procedures, and acceptance responsibilities).
5. Identification of all electronic content sources.
6. Identification of electronic content and/or systems to be converted, replaced, or impacted.
7. Identification of electronic content needed to populate the System so that the Project is a fully functioning system.
8. Identification of all conversion tasks.
9. Schedule of conversion tasks.
10. Conversion environments.
11. Conversion support (system resource requirements, policy, and hardware).
12. Automated and manual conversion system activities.
13. Procedure for continually updating electronic content with additional/new electronic content from the source systems until all the Project sites have been implemented.
14. Identification of and planning for manual support requirements.
15. Identification of control procedures and evaluation criteria.
16. Special training for conversion activities.
17. Conversion testing.
18. Electronic content conversion and load process.
19. Identification and tracking of defects, error handling, and audit requirements.
20. Backup and recovery of converted electronic content, including disaster recovery requirements and methods for returning to State.
21. Procedure to review and compare the electronic content from each State's legacy system with the converted electronic content in the "To Be" System. These reviews shall be conducted, at a minimum, by functional area with any resulting discrepancies documented and fully explained for the approval of the State.
22. Inventory of electronic content from the legacy system that are successfully converted to those in the "To Be" System along with electronic content that cannot be converted. For electronic content that cannot be converted include a detailed explanation for review and approval by State.

A.76. <u>Develop Interfaces with State Solutions.</u>

The Contractor shall work with the State and other external entities to re-engineer and standardize interfaces with State internal and external systems to facilitate seamless integration with these systems.

The Contractor shall develop detailed Interface Design Specifications for all interfaces with the Project including, but not limited to, those defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common. For each Project interface, the Contractor shall identify interface files and processing limitations, define the operating environment, including architecture of the system and error control procedures. The Contractor shall ensure that the Project will integrate successfully all interface functionality. The Contractor is responsible for the design and development of interfaces including security and encryption of the data. The Contractor shall perform testing of all interfaces, in accordance with the Test Plans. This process often involves security access and passwords not available to the Contractor and may require coordination with external agency personnel whose systems shall interface with the Project. The Contractor must be able to integrate with the State's instance of Microsoft Exchange.

The Contractor must be able to integrate with the State's provider of Credit Card and Check Processing.

A.77. <u>Create User Documentation.</u>

The Contractor shall create user documentation for the Project in a format to be approved by the State. Electronic and hard copies of documentation shall be provided. The Contractor shall develop a User Manual that features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The User Manual shall be used by the State Acceptance Test team to mirror the production environment and verify manual content. The Contractor shall create user documentation for the Project in a format to be approved by the State. Electronic and hard copies of documentation shall be provided. The Contractor shall develop the Procedure Manual in a format to be determined by the State. The Contractor shall develop a Procedure Manual which features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The Procedure Manual shall document instructions for manual operations and tasks that are performed in direct conjunction with the automated system. It shall address each task performed in a step by step procedure that identifies the action (task to be performed) and the individual with responsibility to complete the action. The Procedure Manual shall be revised with any changes resulting from the State's Acceptance testing and initial user training sessions.

A.78 <u>Warranty</u>.

Contractor represents and warrants that throughout the Term of this Contract ("Warranty Period"), the goods or services provided under this Contract shall conform to the terms and conditions of this Contract. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.

Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, in conformity with standards generally accepted in Contractor's industry.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services.

A.79 <u>Inspection and Acceptance</u>.

The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

B. TERM OF CONTRACT:

B.1. This Contract shall be effective on September 30, 2015 ("Effective Date") and extend for a period of eighty-four (84) months after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

B.2. **Renewal Options.**
This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to three (3) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of one hundred twenty (120) months.

C. PAYMENT TERMS AND CONDITIONS:

C.1. **Maximum Liability.**
In no event shall the maximum liability of the State under this Contract exceed Written Dollar Amount ($Number) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

C.2. **Compensation Firm.**
The payment methodology in Section C.3 of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct or indirect costs incurred or to be incurred by the Contractor.

C.3. **Payment Methodology.**
The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.

a. The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

b. The Contractor shall be compensated based upon the following payment methodology:

The Contractor shall be compensated for said units, milestones, or increments of service based upon the following payment rates.

Total System Cost **This is the total from the RFQ Attachment E - Part-A of the Cost Proposal**		**$(NUMBER)**

The "Total System Cost" stated above shall be paid to the Contractor in installments contingent upon the completion of Project Phase Milestones, as follows:

PROJECT PHASE MILESTONE	**Percentage of Total System Cost to Be Paid**	**PAYMENT AMOUNT**
Project Initiation Phase and Project Management Requirements **(Appendix 6, Tables 1 and 2)**	5%	$[NUMBER]
Business Process Re-engineering, Organizational Change Management, and System Design Phase **(Appendix 6, Tables 3 through 5)**	5%	$[NUMBER]
Implementation Stage 1A **(Appendix 6, Tables 6 through 10)**	15%	$[NUMBER]
Implementation Stage 1B **(Appendix 6, Tables 6 through 10)**	15%	$[NUMBER]
Implementation Stage 2 **(Appendix 6, Tables 6 through 10)**	10%	$[NUMBER]
Implementation Stage 3 **(Appendix 6, Tables 6 through 10)**	10%	$[NUMBER]
Implementation Stage 4 **(Appendix 6, Tables 6 through 10)**	10%	$[NUMBER]
Implementation Stage 5 **(Appendix 6, Tables 6 through 10)**	10%	$[NUMBER
Retainage Period **(6 Months post Stage 5 implementation – Appendix 6, Table 11)**	20%	$[NUMBER]

Post Retainage								
	Year One	**Year Two**	**Year Three**	**Year Four**	**Year Five**	**Optional Year One**	**Optional Year Two**	**Optional Year Three**
Hosting, (includes 250 Licensed TDA Users)	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR
Support and Maintenance (Appendix 6, Table 11 through 12)	$ / YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR
User Licensing Fee for each additional 10 TDA users post retainage period. (*Pro Forma* Contract, Item A.23.b.)	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR

c. The Contractor shall be compensated for changes requested and performed pursuant to Contract Section A 11, without a formal amendment of this Contract based upon the payment rates detailed in the schedule below and as agreed pursuant to Section A 11, PROVIDED THAT compensation to the Contractor for such "change order" work shall not exceed SEVEN PERCENT (7%) of the sum of milestone payment rates detailed in Section C.3.b., above (which is the total cost for the milestones and associated deliverables set forth in Contract Sections A.3. through A.34. If, at any point during the Term, the State determines that the cost of necessary "change order" work would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	$ Amount (per compensable increment)
Project Manager	$ Amount /HOUR
Business Analyst	$ Amount /HOUR
Technical Manager/Lead	$ Amount /HOUR
Developer	$ Amount /HOUR
NOTE: The Contractor shall not be compensated for travel time to the primary location of service provision.	

d. Pro Rata Payments. A "day" shall be defined as a minimum of eight (8) hours of service. If the Contractor provides fewer than eight hours of service in a standard twenty-four hour day, the Contractor shall bill *pro rata* for only those portions of the day in which service was actually delivered. The Contractor shall not bill more than the daily rate even if the Contractor works more than eight hours in a day.

C.4. **Travel Compensation.**
The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.5. **Invoice Requirements.**
The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month and no later than thirty (30) days after goods or services have been provided to the following address:

State Agency Billing Address

a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

(1) Invoice number (assigned by the Contractor);
(2) Invoice date;
(3) Contract number (assigned by the State);
(4) Customer account name: State Agency & Division Name;
(5) Customer account number (assigned by the Contractor to the above-referenced Customer);
(6) Contractor name;
(7) Contractor Tennessee Edison registration ID number;
(8) Contractor contact for invoice questions (name, phone, or email);

(9) Contractor remittance address;
(10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
(11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
(12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
(13) Amount due for each compensable unit of good or service; and
(14) Total amount due for the invoice period.

b. Contractor's invoices shall:

(1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
(2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
(3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
(4) Include shipping or delivery charges only as authorized in this Contract.

c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. **Payment of Invoice.**
A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. **Invoice Reductions.**
The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

C.8. **Deductions.**
The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. **Prerequisite Documentation.** The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation. At the State's option, it may make payments to Contractor by automated clearing house ("ACH") or the State Purchasing Card ("P-Card").

a. The Contractor shall complete, sign, and present to the State:

(1) An "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and

(2) An "Authorization to Receive Payments by Purchasing Card Form" provided by the State. By doing so, the Contractor agrees that payments to the Contractor under this Contract may be made using the State P-Card.

b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

D. MANDATORY TERMS AND CONDITIONS:

D.1. Required Approvals.
The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

D.2. Communications and Contacts.
All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State: Tennessee Department of Agriculture

Name
Address
Email Address
Telephone # Number
FAX # Number

The Contractor:

Contractor Contact Name & Title
Contractor Name
Address
Email Address
Telephone # Number
FAX # Number

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

D.3. Modification and Amendment.
This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials. The State's exercise of a valid Renewal Option or Term Extension does not constitute an amendment so long as there are no other changes to the Contract's terms and conditions.

D.4. Subject to Funds Availability.
The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State

terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

D.5. Termination for Convenience.
The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

D.6. Termination for Cause.
If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity for breach of this Contract.

D.7. Assignment and Subcontracting.
The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.

D.8. Conflicts of Interest.
The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

D.9. Nondiscrimination.
The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

D.10. Prohibition of Illegal Immigrants.

The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment 1, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.

c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.

d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.

D.11. Records.

The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.

D.12. Monitoring.

The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.

D.13. Progress Reports.

The Contractor shall submit brief, periodic, progress reports to the State as requested.

D.14. Strict Performance.
Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.

D.15. Independent Contractor.
The Parties shall not act as employees, partners, joint ventures, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.

D.16 Patient Protection and Affordable Care Act.
The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.

D.17. Limitation of State's Liability.
The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.

D.18. Limitation of Contractor's Liability.
In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for intentional torts, criminal acts, fraudulent conduct, or omissions that result in personal injuries or death.

D.19. Hold Harmless.
The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Contract.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

D.20. HIPAA Compliance.

The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.

b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

D.21. Tennessee Consolidated Retirement System.

Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq*., the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

D.22. Insurance.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified below. The COI shall be provided ten (10) business days prior to the Effective Date and again upon renewal or replacement of coverages required by this Contract. If insurance expires during the Term, the State must receive a new COI at least thirty (30) calendar days prior to the insurance's expiration date. If the Contractor loses insurance coverage, does not renew coverage, or for any reason becomes uninsured during the Term, the Contractor shall notify the State immediately.

The COI shall be on a form approved by the Tennessee Department of Commerce and Insurance ("TDCI") and signed by an authorized representative of the insurer. The COI shall list each insurer's national association of insurance commissioners (also known as NAIC) number or federal employer identification number and list the State of Tennessee, Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 in the certificate holder section. At any time, the State may require the Contractor to provide a valid COI detailing

coverage description; insurance company; policy number; exceptions; exclusions; policy effective date; policy expiration date; limits of liability; and the name and address of insured. The Contractor's failure to maintain or submit evidence of insurance coverage is considered a material breach of this Contract.

If the Contractor desires to self-insure, then a COI will not be required to prove coverage. In place of the COI, the Contractor must provide a certificate of self-insurance or a letter on the Contractor's letterhead detailing its coverage, liability policy amounts, and proof of funds to reasonably cover such expenses. Compliance with Tenn. Code Ann. § 50-6-405 and the rules of the TDCI is required for the Contractor to self-insure workers' compensation.
All insurance companies must be: (a) acceptable to the State; (b) authorized by the TDCI to transact business in the State of Tennessee; and (c) rated A- VII or better by A. M. Best. The Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that the subcontractors are included under the Contractor's policy.

The Contractor agrees to name the State as an additional insured on any insurance policies with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) ("Professional Liability") insurance. Also, all policies shall contain an endorsement for a waiver of subrogation in favor of the State.

The deductible and any premiums are the Contractor's sole responsibility. Any deductible over fifty thousand dollars ($50,000) must be approved by the State. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.
The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

All coverage required shall be on a primary basis and noncontributory with any other insurance coverage or self-insurance carried by the State. The State reserves the right to amend or require additional endorsements, types of coverage, and higher or lower limits of coverage depending on the nature of the work. Purchases or contracts involving any hazardous activity or equipment, tenant, concessionaire and lease agreements, alcohol sales, cyber-liability risks, environmental risks, special motorized equipment, or property may require customized insurance requirements (e.g. umbrella liability insurance) in addition to the general requirements listed below.

The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability Insurance

1) The Contractor shall maintain commercial general liability insurance, which shall be written on an Insurance Services Office, Inc. (also known as ISO) occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises/operations, independent contractors, contractual liability, completed operations/products, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).

2) The Contractor shall maintain bodily injury/property damage with a combined single limit not less than one million dollars ($1,000,000) per occurrence and two

million dollars ($2,000,000) aggregate for bodily injury and property damage, including products and completed operations coverage with an aggregate limit of at least two million dollars ($2,000,000).

b. Workers' Compensation and Employer Liability Insurance

1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:

i. Workers' compensation and employer liability insurance in the amounts required by appropriate state statutes; or

ii. In an amount not less than one million dollars ($1,000,000) including employer liability of one million dollars ($1,000,000) per accident for bodily injury by accident, one million dollars ($1,000,000) policy limit by disease, and one million dollars ($1,000,000) per employee for bodily injury by disease.

2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:

i. The Contractor employees fewer than five (5) employees;

ii. The Contractor is a sole proprietor;

iii. The Contractor is in the construction business or trades with no employees;

iv. The Contractor is in the coal mining industry with no employees;

v. The Contractor is a state or local government; or

vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Professional Liability Insurance

1) Professional liability insurance shall be written on an occurrence basis. This coverage may be written on a claims-made basis but must include an extended reporting period or "tail coverage" of at least two (2) years after the Term;

2) Any professional liability insurance policy shall have a limit not less than one million dollars ($1,000,000) per claim and two million dollars ($2,000,000) in the aggregate; and

3) If the Contract involves the provision of services by medical professionals, a policy limit not less than two million ($2,000,000) per claim and three million dollars ($3,000,000) in the aggregate for medical malpractice insurance.

D.23. Tennessee Department of Revenue Registration.
The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.

D.24. Debarment and Suspension.
The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;

b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;

c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and

d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

D.25. Force Majeure.
"Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.

D.26. State and Federal Compliance.

The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.

D.27. Governing Law.
This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.

D.28. Entire Agreement.
This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.

D.29. Severability.
If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.

D.30. Headings.
Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.

D.31. Incorporation of Additional Documents.
Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:

a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;

b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below);

c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;

d. the State solicitation, as may be amended, requesting responses in competition for this Contract;

e. any technical specifications provided to proposers during the procurement process to award this Contract; and

f. the Contractor's response seeking this Contract.

E. SPECIAL TERMS AND CONDITIONS:

E.1. Conflicting Terms and Conditions.
Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. 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.

E.3. Printing Authorization.
The Contractor agrees that no publication coming within the jurisdiction of Tenn. Code Ann. §§ 12-7-101, et. seq., shall be printed pursuant to this Contract unless a printing authorization number has been obtained and affixed as required by Tenn. Code Ann. § 12-7-103 (d).

E.4. State Ownership of Goods.
The State shall have ownership, right, title, and interest in all goods provided by Contractor under this Contract including full rights to use the goods and transfer title in the goods to any third parties.

E.5. Ownership of Software and Work Products.

a. Definitions.

(1) "Contractor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.

(2) "Custom-Developed Application Software," shall mean customized application software developed by Contractor solely for State.

(3) "Rights Transfer Application Software," shall mean any pre-existing application software owned by Contractor or a third party, provided to State and to which Contractor will grant and assign, or will facilitate the granting and assignment of, all rights, including the source code, to State.

(4) "Third-Party Software," shall mean software not owned by the State or the Contractor.

(5) "Work Product," shall mean all deliverables exclusive of hardware, such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor exclusively for the State during the course of the project using State's money or resources, including Custom-Developed Application Software. If the deliverables under this Contract include Rights Transfer Application Software, the definition of Work Product shall also include such software. Work Product shall not include Contractor-Owned Software or Third-Party Software.

b. Rights and Title to the Software

(1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license granted under this Contract.

(2) All right, title and interest in and to the Work Product, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other

intellectual property and other proprietary rights embodied by and arising out of the Work Product, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Work Product, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Work Product. Contractor and its employees, agents, contractors or representatives shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties.

(3) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license granted under this Contract.

c. The Contractor may use for its own purposes the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of performing under this Contract. The Contractor may develop for itself, or for others, materials which are similar to or competitive with those that are produced under this Contract.

E.6. State Furnished Property.
The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible personal property furnished by the State for the Contractor's use under this Contract. Upon termination of this Contract, all property furnished by the State shall be returned to the State in the same condition as when received, less reasonable wear and tear. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the fair market value of the property at the time of loss.

E.7. Work Papers Subject to Review.
The Contractor shall make all audit, accounting, or financial analysis work papers, notes, and other documentation available for review by the Comptroller of the Treasury or his representatives, upon request, during normal working hours either while the analysis is in progress or subsequent to the completion of this Contract.

E.8. Prohibited Advertising or Marketing.
The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.

E.9. Contractor Commitment to Diversity.
The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to RFQ #32505-00215 (Attachment B, Item B.15) and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.

E.10. Intellectual Property.
The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor

notice of any such claim or suit and full right and opportunity to conduct the Contractor's own defense thereof, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

E.11. Liquidated Damages.

If an event, as described in *Pro Forma* Section A.30 occurs ("Liquidated Damages Event"), the State may assess damages on Contractor ("Liquidated Damages"). The State shall notify the Contractor of amounts to be assessed as Liquidated Damages. The Parties agree that due to the complicated nature of the Contractor's obligations under this Contract it would be difficult to specifically designate a monetary amount for Contractor's failure to fulfill its obligations regarding the Liquidated Damages Event as these amounts are likely to be uncertain and not easily proven. Contractor has carefully reviewed the Liquidated Damages contained in *Pro Forma* Section A.30 and agrees that these amounts represent a reasonable relationship between the amount and what might reasonably be expected in the event of a Liquidated Damages Event, and are a reasonable estimate of the damages that would occur from a Liquidated Damages Event. The Parties agree that the Liquidated Damages represent solely the damages and injuries sustained by the State in losing the benefit of the bargain with Contractor and do not include any injury or damage sustained by a third party. The Contractor agrees that the Liquidated Damages are in addition to any amounts Contractor may owe the State pursuant to the indemnity provision or any other sections of this Contract.

The State is not obligated to assess Liquidated Damages before availing itself of any other remedy. The State may choose to discontinue Liquidated Damages and avail itself of any other remedy available under this Contract or at law or equity.

E.12. Partial Takeover of Contract.

The State may, at its convenience and without cause, exercise a partial takeover of any service that the Contractor is obligated to perform under this Contract, including any service which is the subject of a subcontract between Contractor and a third party (a "Partial Takeover"). A Partial Takeover of this Contract by the State shall not be deemed a breach of contract. The Contractor shall be given at least thirty (30) days prior written notice of a Partial Takeover. The notice shall specify the areas of service the State will assume and the date the State will be assuming. The State's exercise of a Partial Takeover shall not alter the Contractor's other duties and responsibilities under this Contract. The State reserves the right to withhold from the Contractor any amounts the Contractor would have been paid but for the State's exercise of a Partial Takeover. The amounts shall be withheld effective as of the date the State exercises its right to a Partial Takeover. The State's exercise of its right to a Partial Takeover of this Contract shall not entitle the Contractor to any actual, general, special, incidental, consequential, or any other damages irrespective of any description or amount.

E.13. Unencumbered Personnel.

The Contractor shall not restrict its employees, agents, subcontractors or principals who perform services for the State under this Contract from performing the same or similar services for the State after the termination of this Contract, either as a State employee, an independent contractor, or an employee, agent, subcontractor or principal of another contractor with the State.

E.14. 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 and/or procure 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.

E.15. <u>Survival.</u>

The terms, provisions, representations, and warranties contained in this Contract which by their sense and context are intended to survive the performance and termination of this Contract, shall so survive the completion of performance and termination of this Contract.

IN WITNESS WHEREOF,
Contract Name:

CONTRACTOR SIGNATURE **DATE**

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

TENNESSEE DEPARTMENT OF AGRICULTURE:

JULIUS JOHNSON, COMMISSIONER **DATE**

***Pro Forma* ATTACHMENT 1**

(Fill out only by selected Contractor)

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	
FEDERAL EMPLOYER IDENTIFICATION NUMBER (or Social Security number)	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind Contractor. If said individual is not the chief executive or president, this document shall attach evidence showing the individual's authority to contractually bind Contractor.

PRINTED NAME AND TITLE OF SIGNATORY

DATE OF ATTESTATION

Pro Forma ATTACHMENT 2

(Fill out only by selected Contractor)

SAMPLE LETTER OF DIVERSITY COMMITMENT

(Company Letterhead/Logo)

(Address)
(Date)
(Salutation),

(Company Name) is committed to achieving or surpassing a goal of (numeral) percent spend with certified diversity business enterprise firms on State of Tennessee contract # (Edison document #). Diversity businesses are defined as those that are owned by minority, women, small business and Tennessee service-disabled veterans which are certified by the Governor's Office of Diversity Business Enterprise (Go-DBE).

We confirm our commitment of (percentage) participation on the (Contract) by using the following diversity businesses:

(i) Name and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veteran) of anticipated diversity subcontractors and suppliers:
_____

(ii) Participation estimates (expressed as a percent of the total contract value to be dedicated to diversity subcontractors and suppliers):
_____%.

(iii) Description of anticipated services to be performed by diversity subcontractors and suppliers:

_____

_____

We accept that our commitment to diversity advances the State's efforts to expand opportunity of diversity businesses to do business with the State as contractors and sub-contractors.

Further, we commit to:

1. Using applicable reporting tools that allow the State to track and report purchases from businesses owned by minority, women, Tennessee service-disabled veterans and small business.

2. Reporting quarterly to the Go-DBE office the dollars spent with certified diversity businesses owned by minority, women, Tennessee service-disabled veterans and small business accomplished under contract # (Edison number).

(Company Name) is committed to working with the Go-DBE office to accomplish this goal.

Regards,

(Company authority – signature and title)

TERM	DEFINITION
Acceptance Criteria	The criteria defining the level of functionality and performance at which the deliverable/product and/or document need to perform/provide the State to consider the product/deliverable or part of the product complete. Acceptance Criteria will be defined in the greed upon Acceptance Management Plan.
Account Clerk	The cashier who receipts the monies received by the TDA.
Ag Inputs - Feed, Seed, Fertilizer, Lime	This program area regulates commercial animal feeds, commercial fertilizers, agricultural and vegetable seed and agricultural lime. This includes the issuance of permits or licenses, inspection of establishments, storage facilities, and manufacturing facilities, sample collection for laboratory testing, and fee collection for inspections or assessments. They also ensure compliance with the Federal Seed Act and federal laws regulating commercial feeds. Product labeling is reviewed and samples are obtained in the field. Samples are analyzed in house to ensure label guarantees are met and that standards of quality expected by the customer are achieved. This program area also administers the TN Commodity Indemnity Fund (CIF) that establishes a safety net for grain producers by creating an Indemnity Fund and requiring licensing, bushel assessments and sureties from commodity buyers.
Agency or Agencies	The State of Tennessee, acting by or through one or more departments, boards, commissions, offices or institutions of the State of Tennessee.
Alert	A flag which may be added to a license to indicate problems (i.e. disciplinary, payment), miscellaneous notes or an additional piece of information. The license alerts are displayed during related license maintenance and application processes.
Animal Health	This program area is responsible for the programs aimed at preventing, controlling and eradicating certain infectious or communicable diseases of livestock and other domestic animals. Activities include administering eradication programs for brucellosis, tuberculosis, scrapie, and pseudo rabies along with the control program for equine infectious anemia. Samples are collected and submitted for analysis and results are posted into the system. This program area provides oversight for the National Poultry Improvement Plan in Tennessee. This program area is also charged with the responsibility of enforcing laws and rules regulating interstate and intrastate movement of animals.
Apiary	This program ares is responsible for the recording of apiaries within the State of Tennessee by requiring that each apiary must be properly registered, with its' appropriate geographical coordinates. These coordinates are logged so that individuals and businesses within the State can notify apiary owners of their intent to spray pesticides, and so that they are only dispersed during hours in which the affected hives are dormant. This program area is also responsible for notifying apiary owners of the outbreak of American Foulbrood, a disease that affects apiaries,

TERM	DEFINITION
	and screening apiaries in close proximity to an outbreak to insure that they are not infected. This program area maintains a list of known individuals and businesses that assist in swarm removal and relocation.
Applicant	A person, individual, corporation, LLC, or partnership applying for a license or permit from the TDA.
Application	Submission of specified information and fees (if required), as a request for approval to conduct a regulated activity. License application is a general term that also applies to permits, certification, registrations, education and educational providers. Not all license applications lead to approval as they may not ultimately be approved by the regulating authority.
Application Fee	Monies required by the State in order to complete the processing of an Application.
Assistant Wizard	Help function/guide with external users of TDA system.
Authorized User	Any person(s) who has permission to use TDA and/or various functions pertaining to their specific job requirements
Barcode	An optical machine-readable representation of data, according to State standards.
Batch	Each cashier opens a batch every day in iNovah to receipt monies received by the TDA. Within the batch, every transaction is assigned a transaction number and a receipt number. The total dollar amount of all batches in an office each day should equal the total deposit for that date.
Business Rules	A rule of a business, company, or corporation. It is a rule that defines or constrains some aspect of business and always resolves to either true or false. Business rules are intended to assert business structure or to control or influence the behavior of the business.
Case	Usually related to Compliance functions. This is the identification, tracking, and resolution of a compliance matter and the data and actions associated with it. Examples are the handling and investigation of a complaint, or the investigation and prosecution of professional malpractice, or unlicensed practice.
Cash	Appropriate forms of payment would be a cashier's check, a money order, or a business check.
Cashier (Account Clerk)	The person who uses iNovah to receipt monies received by the TDA.
Central Procurement Office or CPO	The State of Tennessee Central Procurement Office (CPO).
Certification	A document confirming and/or validating a license history of a current or former license holder.
Check 21	The Check 21 Act took effect on October 28, 2004. The law allows the recipient of the original paper check to create a digital version of the original check, a process known as Check truncation, into an electronic format called a "substitute check", thereby eliminating the need for further handling of the physical document.
Complaint	A formal allegation of impropriety against an individual/entity.
Contract	The writing(s) which contain the agreement of the Central Procurement Office (CPO) and the Respondent/Contractor setting forth the total legal obligation between the parties as determined by

TERM	DEFINITION
	applicable rules of law.
Contract Requirements	The tasks and deliverables that the selected contractor will be responsible for once a contract has been executed and approved by the State.
Contractor	A firm that the State contracts with to provide services defined in the RFQ & Pro Forma Contract.
COTS Software Provider	A provider of commercial off the shelf Licensing and Enforcement software, a line-of-business (LOB) software product containing business rules and processes.
Customer	External users utilizing the TDA system to add, change, delete, or inquire. A customer can be a licensee, an applicant, a member of the general public, or other users of the system.
Dairy	This program area is responsible for the inspection of dairy farms, dairy plants, milk transport trucks, dairy and trade product distributors and milk samplers. Samples are collected and specialized laboratory analyses are performed and results are reported. The Contractor shall design the System to integrate with the State's existing system so that sample results will be tied directly back to the inspected facility. A mechanism for integrating data from outside (private) laboratories must also be provided for by the Contractor.
DBA	Doing Business As. This is your trade name.
DBA Change	A business may request to change their "Doing Business As" name, or trade name. Documentation must be submitted and approved prior to any actual change. The license number and expiration date do not change.
Defect	A failure of a configuration, modification, and/or customization of the software to operate in accordance with the Acceptance Criteria or RFQ functional or technical requirements or a failure of the Software to operate in accordance with the Software program documentation.
Deliverable	Any document deliverable, software deliverable or service that the Contractor is required to provide the State under the Contract.
Deliverable Acceptance	The written approval by the State Project Manager or his or her written designee that one or more Deliverables have met all applicable Acceptance Criteria and comply with the terms of the Contract.
Documentation	Refers to various types of document that will have to be prepared by the contractor and provided to the State in a form and format specified by the State. Types of documentation include, but are not limited to, pre and post meeting documentation, system documentation, technical documentation, training documents etc.
Downtime	The period of time in a given month when the System, or any portion thereof, because of failure of any or all software, is not operation in conformance with the defined System Requirements. Down-time shall begin 15 minutes after the Contractor is notified of the issue.
ERP	Enterprise Resource Planning is the State's Edison system. The new system will need to interface with Edison financials for cashiering purposes.
Edison	The State's Enterprise Resource Planning System.
Entity	An individual, group of individuals, business, brand, product or

TERM	DEFINITION
	object that has a unique identity. The applicant that applies for or holds a license or permit. Entity could be an LLC, Corporation, partnership, sole proprietorship etc.
Expiration	When the time period for an issued license or permit is over.
External Miscellaneous Transaction	A licensee, an applicant, a member of the public or any other user of the system who submits and application via the Internet which upon approval, will perform an action and/or amend information related to a specific entity and/or associate license.
External User	Synonymous with customer - a licensee, an application, a member of the general public or other users of the system.
Fees	Costs or payments related to licensing, e.g.: application fees, license/permit fees, renewal fees, education fees, and processing fees.
Final Acceptance	The point in the lifecycle at which the System Implementation is complete for all phases of the system and TDA agrees that the production system has performed for a pre-defined period (Software Production Verification) according to all Acceptance Criteria and System Requirements in the production environment.
Fine	In any case where the TDA is given the power to suspend or revoke any license or permit, they can levy a fine to remedy the matter. Fines are dollar amounts assigned by citations for violations of the rules and regulations or Tennessee Code Annotated.
FIS	Fidelity National Information Services, Inc. is the provider of banking and payments technology for the State of Tennessee. The payments-focused platforms will be used in supporting the State's benefits programs and payment collections. FIS enables the State to easily accept payments for recurring services, such as public utilities, or for one-time fees, fines and citations.
Fiscal Year	The TDA operates on a fiscal year from July 1 through June 30.
Flag	This term is synonymous with alerts and notifications and can have a number of different types which based on the type would trigger a workflow process.
Food Safety	This program area is also responsible for assuring the public of a safe, wholesome and properly represented food supply through permitting and inspection of food establishments, inspection of food products, and performance of specialized laboratory analyses on a variety of food products sold or produced in the State. This program area inspects food manufacturers, food warehouses, and food distributors to ensure wholesome food processing and storage practices. Samples are collected and specialized laboratory analyses are performed and results reported through an external system. Sample results will be tied directly back to the inspected facility. Tobacco Compliance is responsible for inspections that are conducted in retail establishments to ensure compliance with Tennessee statutes prohibiting the sale of tobacco products to persons less than eighteen years of age. Underage youth accompanied by an adult, visit stores and attempt to purchase a tobacco product. Proper packaging and signage are verified. Merchants are notified of the outcome and civil penalties are issued for second or subsequent violations.

TERM	DEFINITION
Food service establishment	(A) Food service establishment means any establishment, place or location, whether permanent, temporary, seasonal, or itinerant, where food is prepared and the public is offered to be served or is served food, including, but not limited to, foods, vegetables, or beverages not in an original package or container, food and beverages dispensed at soda fountains and delicatessens, sliced watermelon, ice balls, or water mixtures; (B) Food service establishment includes places identified in subdivision (A), regardless of whether there is a charge for the food; (C) Food service establishment does not include private homes where food is prepared or served and not offered for sale, retail food store operations other than delicatessens, the location of vending machines or supply vehicles; (D) Food service establishment does not include churches, temples, synagogues or other religious institutions, civic, fraternal, or veteran's organizations where food is prepared, served, transported, or stored by volunteer personnel only on non-consecutive days; provided, however, that the storage of unopened, commercially canned food, packaged bulk food that is not potentially hazardous as defined by department rules and regulations, and dry goods shall not apply for these purposes; (E) Food service establishment does not include grocery stores that may, incidentally, make infrequent casual sales of uncooked foods for consumption on the premises, or any establishment whose primary business is other than food service that may, incidentally, make infrequent casual sales of coffee or prepackaged foods or both, for consumption on the premises. For the purposes of this subdivision (9)(E), infrequent casual sales means sales not in excess of one hundred fifty dollars ($150) per day on any particular day; (F) Food service establishment does not include a location from which casual, occasional food sales are conducted solely in connection with youth-related amateur athletic or recreational activities or primary or secondary school-related clubs by volunteer personnel and that are in operation for twenty-four (24) consecutive hours or less; (G) Food service establishment does not include a catering business that employs no regular, full-time employees, the food preparation for such business is solely performed within the confines of the principal residence of the proprietor, and the catering business makes only occasional sales during any thirty-day period; and (H) Food service establishment does not include a house or other residential structure where seriously ill or injured children and their families are provided temporary accommodations in proximity to their treatment hospitals and where food is prepared, served, transported or stored by volunteer personnel; provided, that the

TERM	DEFINITION
	house or structure is supported by a 501(c)(3) organization, as defined in 26 U.S.C. 501(c)(3), that has as a component of its mission the support of programs that directly improve the health and well-being of children;
GIS	Geographic Information System.
International Standards Organization	ISO27001 ▪ An internationally recognized structured methodology dedicated to information security. ▪ A management process to evaluate, implement and maintain an information security management system. ▪ A comprehensive set of controls comprised of best practices in information security. ▪ Applicable to all industry sectors. ▪ Emphasis on prevention.
iNovah	The cashiering system utilized by the State of Tennessee. Each transaction is numbered and assigned a specific receipt number, and transactions each day are grouped into a batch for each cashier. Batches are dated the day they are to be deposited, and the total of all batches in an office should equal the total of that day's deposit for each office, as well as the total on the mail log.
Inspections	An inspection will be conducted by a TDA agent after a new application has been reviewed by the TDA office. The agent will bring a copy of the rules and regulations. They will also verify that the establishment meets the qualifications of the type of permit applied for, and in some cases determine the required license fee. Renewal inspections are done prior to the expiration of a license, and routine inspections can be done periodically during the license term.
Internal User	Users of the licensing system who work for a state agency participating in the licensing project. These users generally process, review or manage information provided by license applicants or other non- state people who use the system (external users).
License	The TDA issues several licenses to qualified applicants. The license must be prominently posted in a conspicuous location in your licensed establishment.
License Application	Submission of specified information and fees (if required), as a request for approval to conduct a regulated activity. License application is a general term that also applies to permits, certifications and registrations as well as licenses. Not all license applications lead to the approval and granting of a license, permit, certification or registration as they may not ultimately be approved by the regulating authority.
License Fee	Also referred to as a privilege tax.
License Status	The state of a license at a particular time, noted such as current, cancelled, expired, null and void, suspended, revoked, etc.
Licensee	Any establishment that holds a license from the TDA.
Mail Log	Any mail, Fed Ex, UPS, or other incoming type of mail that includes any form of money must be opened with two individuals present, and logged into a mail log which notes who it applies to, when it was received, and what check number is on a check or money

TERM	DEFINITION
	order.
Mandatory Requirements	Requirements that the Respondent must meet in order to be eligible for contract award
Miscellaneous Transaction	A transaction which performs and action and/or amends data for a specific entity and/or associated license. These transactions may be “one off” transactions as defined by business rules.
Monthly Report	At the end of each month, each office compiles a report of all licenses issued and voided during that month.
Notification	An official announcement about an action that has been taken or will be taken relating to a license record or business process.
Payment Card Industry	The Payment Card Industry Data Security Standard (PCI DSS) was created by the major credit card issuers, and applies to companies that accept, store process and transmit credit cardholder data. When it comes to data center operators, they should prove they have a PCI compliant environment with an independent audit.
Pesticides	This program area regulates the use, misuse, distribution and sale of pesticides across the state. This includes the issuance of certificates (i.e., Commercial and Private applicator certifications, licenses, charter companies, restricted use product dealers, and Worker/Handler), registration of all pesticide products sold in the state, conducting inspections of Pest Control companies, investigating complaints regarding pesticide related health and/or environmental issues, and ensuring compliance with Federal Groundwater, Endangered Species and Worker Protection Acts. The Pesticide section is also responsible for administering the licensing examinations, approves industry sponsored training and applies CEUs to records for all of those applicators who hold a current certification in the state.
Permit	Permits are generally issued to individuals or business. The individual holder of the permit is responsible for renewal of a permit prior to the expiration of that permit and the permit is the sole property of such individual holder. There is no grace period for an expiring permit.
Permit Term	The length of time that a license is current and valid.
Petroleum	This program area monitors the quality of petroleum products conveyed for commercial consumption in Tennessee. Commercial facilities are inspected annually for compliance with applicable laws and regulations. Inspections include water bottoms in storage tanks, dispenser labeling requirements, and field tests such as gasoline octane and diesel fuel flash point. In addition, samples of the product are collected and sent to a central laboratory for extensive analysis. All inspection and laboratory results are entered into a computer system and are linked to the establishment where they are collected.
Plan view	The State's Enterprise Portfolio Management tool.
Plant Certification	This program area is responsible for the inspection and certification of all firms in Tennessee dealing in production and sales of rooted plant materials. All nurseries are required to be inspected a minimum of once a year and greenhouses are inspected twice a year. Retail sellers of plant materials are audited once every three years. Other functions include special inspections for various compliance agreements and issuance of Phytosanitary Certificates (Both Federal & State). Certificate holders are subject to civil penalties for violating the Plant Pest Act and any of it associated

TERM	DEFINITION
	rules. Charges for requested Nematode samples occur for nurseries that ship to various countries. These products are inspected for proper labeling and sampled / analyzed to ensure products are as represented by product label and meet standards set by state or federal requirements.
Program Area	A Program Area consists of a set of operational activities under the general supervision of a Program Administrator. The Consumer and Industry Services Division is comprised of the following Program Areas: Ag Inputs, Animal Health, Apiary, Dairy Inspection, Food Safety, Pesticide Services, Petroleum, Plant Certification, and Weights & Measures.
Prominent	Standing out so as to be seen easily; particularly noticeable.
Policy and Procedures	The manual to provide guidance for internal regulations and procedures for TDA employees.
Renewal Inspection	Prior to the expiration of a license, a TDA inspector will conduct a renewal inspection at the place of business. He will either leave the paperwork for the renewal, or direct them to the forms online that they need to submit. The inspector will verify that the establishment continues to meet the legal requirements of their license and the amount of their renewal license fee. He also checks for the proper, unexpired employee permits and verifies that all signs and licenses are properly posted.
Renewals	Licenses are issued to expire based on business rules from the date of issue, or on a calendar year for certain types of licenses. Before a license expires, if an establishment wishes to keep their license, they must submit a renewal application to the TDA along with any required supporting documents and the renewal license fee. A license cannot be renewed until all documents are submitted, all citations are paid, and any outstanding issues are remedied.
Replacement Card	If an individual loses their employee permit, they can apply to the TDA for a replacement permit by submitting the appropriate form, either online, or through the mail.
Respondent	The entity that submits materials to the State in accordance with these instructions.
Response	The material submitted by the respondent in answering the solicitation.
Responsible Bidder or Responsible Respondent	A Bidder that is determined to have financial and organizational capacity, legal authority, satisfactory previous performance, skill, judgment and integrity, and that is found to be competent, reliable and experienced, as determined by the Central Procurement Office.
Responsive Bidder or Responsive Respondent	A Bidder or Respondent meeting the specifications or requirements prescribed in the Proposal Document or solicitation, as determined by the Central Procurement Office.
Request for Qualifications or RFQ	A type of Proposal Document that is used for procurements where factors in addition to cost are considered and weighted in awarding the contract.
Return Log	Any monies received by the TDA that are incorrect or not required should be logged onto a return log before being returned to the sender, noting the date they were received, who sent them, what type of payment they were, the date returned and the check number.
Revocation	Cancellation or withdrawal of a license permit, power, privilege or

TERM	DEFINITION
	act.
Routine Inspection	Agents usually try to conduct at least one routine inspection during a license year. Routine inspections are usually unexpected by the licensee. Generally the agent verifies that the establishment continues to meet their legal requirements, and that all licenses are properly posted. If the TDA receives a complaint on an establishment that needs investigation, an agent may conduct additional routine inspections at that establishment.
Rules & Regulations	The Tennessee Department of Agriculture has the authority to promulgate rules and regulations pertaining to license issued by TDA. These rules can be found on the TDA website at http://www.tn.gov/sos/rules/0080/0080.htm
Schedule of Events	The list of critical dates and actions included in the introductory materials.
Service Organization Control	**SOC 2 Type 2** This report and audit is completely different from the previous SOC 2 measures controls specifically related to IT and data center service providers. The five controls are security, availability, processing integrity (ensuring system accuracy, completion and authorization), confidentiality and privacy. Type 2 – Includes everything in Type 1, with the addition of verification of an auditor's opinion on the operating effectiveness of the controls.
	SOC 3 This report includes the auditor's opinion of SOC 2 components with an additional seal of approval to be used on websites and other documents. The report is less detailed and technical than a SOC 2 report.
Software Product	The software, including configurations and customizations, delivered to the State in accordance with the resulting Contract.
Software Product Verification	The pre-defined period during which the State monitors and verifies that system functions and system performance continue to meet Acceptance Criteria in the production environment.
Solicitation Coordinator	State of Tennessee representative for whom all communications relating to this solicitation shall be directed to.
Standard Manufacturer or Manufacturer's Warranty	An agreement which generally warrants against defects in workmanship or materials for a specified period of time after item purchase or shipment. The warranty shall be included in any sales agreement between the Contractor and the State for the purchase of goods and services specified in this RFQ. The length and terms of the warranty shall be specified and detailed before purchase.
State	State of Tennessee.
Status	The state of a TDA record [license/permit/education] at a particular time to be defined by business rules.
Subcontractor	Any individual or other legal entity, (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) that has entered into a contract, express or implied, for the performance of a portion of a Contract with a Contractor.
System Acceptance	The period in the project management lifecycle at which every aspect of the application phase being developed, along with any supporting data conversion routines and system utilities, is thoroughly validated ty by the TDA prior to proceeding with the System Implementation.

TERM	DEFINITION
System Implementation	The period in the project management lifecycle where the system is moved from a test environment to the live production environment and the system starts to be used for real business transactions.
System Requirement	A defined business function that is a required component of TDA system, specified in the RFQ and Appendix 6 Functional and Technical Requirements, as well as any detailed requirements established during the Business Process Reengineering and System Design phase of this project.
Surrender	When a licensed establishment closes, or no longer wishes to keep their license, they must surrender their license to the TDA. This means they should bring or mail in the actual license to the local TDA office along with a letter stating that they wish to surrender their license. When the TDA receives this, we will void your license.
Suspension	The temporary withdrawal of a license permit or privilege.
TDA	Tennessee Department of Agriculture
T.C.A. (Tennessee Code Annotated)	The Tennessee statutory law. (http://www.lexisnexis.com/hottopics/tncode/)
Transaction	Any activity carried out, performed, managed or conducted by a user of the system.
Transaction Log	A log that contains the history of transactions executed by the system and the user or operator associated with each transaction.
Transfer of Location	TDA licenses can request to transfer their location from one place to another. Appropriate documentation has to be submitted and approved prior to the move.
Unique Identifier	A string of characters that uniquely identifies a wide variety of entity/licensing items guaranteeing uniqueness with the entire system.
User	Anyone who employs the services provided by the system. The user can be an individual visitor to the TDA website, an applicant or licensee, a licensing agency staff member, or recipient of specific content from the system. See also Authorized User.
User Acceptance	Approval by the State that system functions and performance have met Acceptance Criteria after testing in a non-production version of the system.
Validity dates	The date range in which a license/permit/education is valid.
Violation	An incident where a licensee or other entity has broken a law or procedure in connection with their license/permit/education that TDA has been made aware of.
Weekly Report	Each week the TDA office issues a report showing all new licenses issued in the state, all voided licenses in the state, and all changes with licenses in the state for the prior week.
Weights & Measures	This program area monitors all commercial weighing and measuring devices in Tennessee. The devices inspected and tested include liquid fuel dispensers, bulk meters, LPG meters, and scales (small, medium, and large capacity). Inspections include net weight and price scanner verifications. The metrology laboratory calibrates volume and mass standards submitted to the laboratory; invoices are generated for the laboratory services provided.
Work Breakdown Structure (WBS)	A graphical representation of the hierarchy of project deliverables and their associated tasks. As opposed to a project Schedule that is calendar-based, a WBS is a deliverable-based, and written in business terms.
Workflow	Sequence of tasks. A workflow describes the order of a set of tasks

TERM	DEFINITION
	performed to complete a given procedure within an organization
Workflow Process	A series of steps through which work is routed.
Weekly Report	Each week the TDA office issues a report showing all new licenses issued in the state, all voided licenses in the state, and all changes with licenses in the state for the prior week.
Workflow System	A system which manages and defines a series of tasks within an organization to produce a final outcome(s)

	T.C.A.	Number
Weights & Measures		
Weighmaster License	47-26-1001	1,869
Certified Public Weigher Lic.	47-26-801	1,085
Serviceman Registration	47-26-1110	986
Pumps	47-26-909	
regular flow 1 - 6 pumps		759
regular flow 7 - 18 pumps		1,339
regular flow 19 - 36 pumps		1,860
regular flow 37- 54 pumps		454
regular flow 55 - 78 pumps		73
79 or more		9
High flow 1 - 6 pumps		234
6 or more		47
Scales (small)	47-26-909	
establishments with 1 - 5		3,370
establishments with 6 - 20		527
establishments with more than 20		200
Scales (large)	47-26-909	
1 to 2 large scales		935
3 or more larges scales		531
LPG/Bulk Meter	47-26-909	2,462
Bulk Mass Flow Meters	47-26-909	10
Retail CNG/LNG	47-26-909	10
Food & Dairy		
Meat & Poultry Inspection	53-7-219	
Custom Slaughter License	53-7-220	319
Vending Machine License	53-12-104(b)	
Egg License	53-2-109	56
Retail Food Store License	53-8-214	9,130
Food Manufacturers	53-1-208(3)(A)	1,304
High Risk		121
Medium Risk		418
Low Risk		687
Food Warehouses	53-1-208(3)(B)	512
High Risk		3
Medium Risk		133
Low Risk		373
Certificate of Free Sale	53-1-208(4)	797
Frozen Dessert Mfg. License	53-3-106(a)(1)	4
Distributor's Frozen Dessert Lic.	53-3-106(a)(4)	17
Distributor's Dairy Product Lic.	53-3-106(a)(4)	28
Dairy/Trade Products Mfg. Lic.	53-3-106(a)(2)	23
Dairy/Trade Products Registration	53-3-107(a)(1)	1,447
Milk Tester's License	53-3-105(b)	55

Milk Sampler's License	53-3-105(a)	196
AG Inputs		
Vendor to Wholesale Seed Lic.	43-10-118(a)(1)	105
Retail Agriculture Seed Lic.	43-10-118(a)(2)	2,833
Wholesale Agriculture Seed Lic.	43-10-118(a)(3)	185
Seedsman License		387
Seed Unit Fee >3000		3,961,714
Feed Tonnage (GF)	44-6-109, 44-6-104	
Feed Facility License	44-6-104(b)	1,388
Feed Tonnage Fee > 500 tons		6,548
Fertilizer Brand Registration	43-11-104	6,598
Fertilizer License (+tonnage fee + brand fee)		356
Tonnage Fee >1000 tons		576
Brand Fee >10 brands		904
Ag Liming Materials (license + tonnage fee)	43-11-405	57
Tonnage Fee >1000 tons		576
Plant Certification		
Nematode Sample Analysis	43-1-703(f)(7)	14
Plant Certificates - Nursery	43-1-703(f)(8)	653
Plant Certificates - Greenhouse	43-1-703(f)(8)	293
Plant Certificates - Plant Dealer	43-1-703(f)(8)	2,293
Phytosantitary Certificates	43-1-703(f)(15)	1,884
Pesticides		
Pesticide Dealer License	43-1-703(f)(11)	325
Pest. Applicator Certification Fee	43-1-703(f)(4)	5,070
Pesticide Product Registration	43-1-703(f)(13)	13,163
Special Local Need	43-1-703(f)(18)	2
Aerial Applicator	43-1-703(f)(1)	91
Aerial Decal	43-1-703(f)(2)	81
Pest Control Operator Fee	43-1-703(f)(9)	1,379
Pest Control Exam	43-1-703(f)(6)	365
Pesticide Private Applicator	43-1-703(f)(16)	688
Animal		
Certificate of Brand Registration	47-7-202 & 204	80
Livestock Dealer License	44-10-203	111
Livestock Market License	44-11-104	17
Baby Chick Law	44-16-202	139

Section	Report	STAGE REQUIRED
Agricultural Inputs		
	Ad Hoc Report	2
	Anhydrous Ammonia Renewal status	2
	Commercial Feed Samples by Dealer	2
	Commercial Feed Samples by Manufacturer	2
	Commercial Fertilizer Samples by Dealer	2
	Commercial Fertilizer Samples by Manufacturer	2
	Commercial Lime Samples by Dealer	2
	Commercial Lime Samples by Manufacturer	2
	Commercial Seed Samples by Dealer	2
	Commercial Seed Samples by Manufacturer	2
	Feed Licenses	2
	Feed Tonnage Detail -date firm specified	2
	Feed Tonnage Non-reporters	2
	Feed Tonnage Summary- date firm specified	2
	Feed Tonnage Top 50 Producers	2
	Feed Tonnage Top Producers- date type	2
	Feed Not Reporting	2
	Fertilizer Data – Info retrieved from TFTRS	2
	Inspector Performance Report	2
	Lime facility renewal - tonnage status	2
	lime tonnage summary by county	2
	lime tonnage summary by region	2
	Recent Samples	2
	Recent Violations Report (Adjustable Range)	2
	Seed List	2
	Seed Reporting companies and licenses	2
	State Report	2
	Upcoming Inspections	2
Civil Penalties		
	Civil Penalties: Issued for Previous Week	1B
	Civil Penalties: Pending	1B
	Civil Penalties: Delinquent	1B
	Civil Penalties: Paid	1B
	Civil Penalties: Delinquent Critical Item Letters	1B
Dairy		
	Broken Seal Tracking	1B
	Dairy Inspection Summary Need for plants also	1B
	Dairy Permit Summary	1A
	Distributor's License	1A
	Double Debit and Triple Debit Report (Need for plants also)	1A
	Equipment tests for plants	1A
	Farm History Report	1A
	Farm Inspection Detail Report	1A
	Farm Inspection Summary Report	1A
	Farm listing Report	1A

Section	Report	STAGE REQUIRED
	Farms and Plants Requiring Water/Glycol/Sweetwater Sample	1B
	Frequencies of Inspections Done	1B
	Industry Emergency Sealer Personnel Tracking	1B
	List Number of Active Farms by BTU	1A
	Milk Sample Results Upload Rejection Report	1A
	Milk Sample Summary	1B
	Notification of Failure to Receive Surety Bond	1B
	Producer Reinstatement Status Report	1B
	Random Survey Report	1B
	Sample Deficiency Report Need for plants also	1B
	Sampler / Hauler tracking for recertification/permitting	1A
	Sampler Mailing labels	1B
	Sampling Surveillance Officer Tracking (SSO) / Delegate Sampling Surveillance Officer (DSSO)	1A
	Somatic Cell Info-Qualify % Information	1A
	Surety Bond Tracking	1B
	TDA Grade A Dairy Farm & Plant Inspection Report (Past 24 Months)	1B
	Truck Permit/Inspection Tracking	1B
	Warning Status Report Need for plants also	1B
	Warning/Penalty Count/Suspension/Penalty List	1B
Dairy- Other Program Areas		
	Eggs- Annual Permit	1B
	Eggs - Fee Reconciliation	1B
	Eggs - Inspection Report	1B
	Meats (Custom Slaughter or Meat Processors) -Annual Permit	1B
	Meats (Custom Slaughter or Meat Processors)- Fee Reconciliation	1B
	Meats (Custom Slaughter or Meat Processors) -Inspection Report	1B
Food Safety		
	Food Establishments By County Report	1A
	Food Establishment Uninspected Report	1A
	Food Establishment Profile Detail Listing	1A
	Retail Food Establishment to Sample	1A
	Civil Fines Summary Report	1B
	Previous Inspection Data	1B
	Weekly Food Reports: Emergency Contact List	1B
	Weekly Food Reports: Profile list	1B
	Weekly Food Reports: New Profile listing	1B
	Weekly Food Reports: Renewal Report	1B
	Weekly Food Reports: Device Only Establishments	1B
	Areas Closed	1B
	Seizures and Condemnations	1B
Food Safety- Tobacco		
	Tobacco: Establishment Compliance	1B

Section	Report	STAGE REQUIRED
	Tobacco: Establishment History	1B
	Tobacco: Complete Report	1B
	Tobacco: Incomplete Report	1B
	Tobacco: Sign Posted Recap	1B
	Tobacco: Enforcement Summary (By Year)	1B
	Tobacco: Enforcement Summary (By Month/Year)	1B
	Tobacco: Compliance	1B
	Tobacco: Enforcement Fines	1B
	Tobacco: Generated Sign Fines	1B
	Tobacco: Yearly Report	1B
General Financial		
	Financial: CD Report	1B
	Financial: Revenue	1B
	Financial: Account Detail Report	1B
	Financial: Register Report	1B
	Financial: Refund Report	1B
Pesticide- Certification Testing		
	History of activity of taking license and certification exams	5
	Refunds requesting for testing	5
	Report by location, category of license and certification exam scheduled and taken	5
	Report by name, address, city, state, zip, phone and email address	5
	Report by pass, fail, score and no show	5
	Report fees paid for certification exams requested and by category of exam	5
	Report number missing the questions administered (item analysis)	5
	Report number of company employees taking test for the 1st time vs repeat request	5
	Report number of confirmations sent and returned	5
	Report number of days blocked out for test not to be administered	5
	Report number of seats filled and available for testing	5
	Report number requesting special testing sessions (written, category and by date)	5
	Report of questions missed with the correct and incorrect answer	5
Pesticide- Chartered Pest Control Companies		
	History of Activity for all companies	5
	Report by name, address, city, state, zip, county, phone number and email address	5
	Report Notice of Violation and Enforcement Actions issued by rule and regulation	5
	Report number of applicators connected to a charter including licenses and certifications	5
	Report number of refunds requested and dollar amount	5
	Report of all pest control companies that have paid renewal fees and civil penalties, those not paid and delinquent	5
	Report of companies inspected and needing to be inspected	5
	Report of companies out of business and brought out	5
	Report of current and expired bond and insurance	5
Pesticides- Complaints		
	History of Activity	5
	Report number of complaints assigned by inspector and supervisor and who	5

Section	Report	STAGE REQUIRED
	initiated the complaint	5
	Report number of complaints by type, including illegal operators	5
	Report number of complaints received, by name, address, city, state, zip, county, phone and email address	5
	Report number of days to close complaint	5
Pesticides – Enforcement		
	EPA Reports and Performance Measures	5
	History of Activity	5
	Report by applicator, company, ID number, name, address, city, state, zip, county phone, and email address	5
	Report civil penalties paid, owed and delinquent	5
	Report number of administrative hearings conducted, date, reason, and outcome	5
	Report number of days from start to close inspections	5
	Report number of informal discussions held, date, results, date case closed, rule and Regulation	5
	Report number of Notice of Violation and Enforcement Actions issued by rule and regulation and by inspection type	5
	Report number of routine, follow-up, complaint, inspection type and total number of Inspections	5
	Report number of samples collected, analyzed, sample type and results	5
Pesticides – Pesticide Applicators (Commercial, Private, Licensed, including Limited Herbicide Applicator (LHA))		
	EPA reports and CPARD (Certification Plan and Reporting Database)	5
	History of activity for all applicators	5
	Insurance for Aerial	5
	Renewals for all licensed applicators	5
	Report by name, address, city, state, zip, county phone and email address	5
	Report categories of certifications and license issued, current and expired	5
	Report decals assigned to Aircraft & Aircraft number	5
	Report fees and civil penalties paid, owed and delinquent	5
	Report Notice of Violation and Enforcement Actions Issued by rule and regulation	5
	Report number of certification cards issued	5
	Report number of recertification letters sent to private applicators	5
	Report number of refunds requested and dollar amount	5
	Report of applicators deceased and removed from chartered companies	5
	Report of applicators with accrued CEU's and needing CEU's by category of certification	5
Pesticides- Products and Manufacturers		
	Fees and civil penalties paid, owed and delinquent	5
	History of activity	5
	Renewals for all products expiring on a yearly basis	5
	Report by ID number assigned, type, use, EPA Registration number, discontinued, RUP (Restricted Use Pesticide) current and expired	5
	Report by manufacturer name, address, city, state, zip, phone, email and state contact	5
	Report Notice of Violation and Enforcement Actions issued by rule and regulation	5
	Report number of refunds requested and dollar amount	5
Pesticides- Restricted Use Pesticide Dealers		

Section	Report	STAGE REQUIRED
	Category 12 Pesticide Dealer current and expired listed by name and ID number assigned	5
	EPA reports	5
	History of activity for all dealers	5
	Report by name, address, city, state, zip, county, phone and email address	5
	Report fees and civil penalties paid, owed and delinquent	5
	Report inspected and needing to be inspected	5
	Report Notice of Violation and Enforcement Actions issued by rule and regulation	5
	Report number of refunds requested and dollar amount	5
	Report of dealers out of business	5
Pesticides-WPS-Worker Protection Standard		
	EPA reports and CPARD (Certification Plan and Reporting Database)	5
	History of Activity	5
	Report category of certification trainer holds and expiration date	5
	Report persons conducting training by name, address, city, state, zip, county, phone number and email address	5
	Report worker and handlers current and expired	5
Plant Certification		
	Certified Sod Certificate	3
	Educational Organization Certificate	3
	Florist Dealer Certificate	3
	Greenhouse Certificate	3
	Hemp License Certificate	3
	Hobbyist Greenhouse Certificate	3
	Hobbyist Nursery Certificate	3
	Landscaper Certificate	3
	limited Plant Dealer Certificate	3
	Native Wild Plant Dealer Certificate	3
	Nursery Certificate	3
	Plant Dealer Certificate	3
	Sweet Potato Seed Dealer Certificate	3
	Sweet Potato Slip Certificate	3
Point to Point		
	Inspector Task Profile Report for Section	1B
	Program Activity Summary for Section	1B
	Program Summary for Section	1B
	Point to Point by Inspector	1B
	Point to Point (PTP) Reporting	1B
	Point to Point- Day (Dups filtered out)	1B
Revenues		
	Revenue: Unpaid Fee Summary	1B
System Wide Reports		
	Quarterly: Performance Report	1B
	Quarterly: Frequency of Violations	1B
	Quarterly: Facility Statistics Report	1B
	Quarterly: Scoring Level and Workload	1B

Section	Report	STAGE REQUIRED
Tobacco Compliance		
	Mental Health Report	1B
	Tobacco Report	1B
Weight and Measures / Petroleum Quality		
	Annual Report on the Quality of Kerosene and Motor Fuel in Tennessee- (by FY)	1A
	Bulk Meter Inspection Summary	1B
	Certificate of Analysis Report- By Product Types and/or Grades	1A
	Checkweighing Report	1B
	Checkweighing Report- By County, By Inspector, By Type	1B
	Checkweighing/Price Verification Detail	1B
	Consumer Complaint Report (Various parameters)	1A
	Device Inspection Summary	1B
	Establishments With Devices Detail	1A
	Establishments With Devices Summary	1A
	Fines (Various parameters)	1A
	LPG Meter Inspection Summary	1B
	Meter/Inspection Summary Report - (Meter Type)	1B
	Notice of Violation and Issuance of Enforcement Action	1A
	Product Violation Analysis Report	1A
	Price Verification Report	1B
	Price Verification Report - By County, By Inspector	1B
	Pump Inspection Summary	1B
	Report of Petroleum Storage Tanks Testes	1B
	Report of Weighing and Measuring Devices Tested (BNK-NOZ)	1B
	Report of Weighing and Measuring Devices Tested (Scale)	1B
	Report of Weighing and Measuring Devices Tested (Serial)	1B
	Report of Weighing Devices Tested	1B
	Service Agencies by Type	1A
	Statistical Reports	1B
	Stop Sale (Various parameters)	1A
	Summary of Establishments with Devices	1A
	Uninspected Establishments	1A
	Uninspected Establishments Devices	1A
	Violation Analysis Report	1A
	Weights and Measures Statistical Report	1B
	Weights and Measures Numbers Report	1B
	Violation Analysis Report	1A

Section	Form	Form ID
Agricultural Inputs		
	Ag Establishment Inspection Report	AG-0605
	Certification of Grain Payments Within 30 Days of Delivery	
	Chain of Custody Record for Samples	AG-0583
	Extension Request	
	Generic Field Stop Sale & Seizure Notice	AG-0483
	Indemnity Fund Monthly Report	
	Nonresident Exemption	AG-0487
	Not a Purchaser of Grain from Producers	
	Proof of Claim	
	Refund of Grain Indemnity Fund Assessment	AG-0486
	Sample Report	AG-0488
	Tennessee Commodity Producer Indemnity Fund Monthly Report	
	Tennessee Grain Indemnity Fund - Proof of Claim	
Animal Health		
	Application for Livestock Brand Registration	AG-0052
	Application for Tennessee Baby Chick Sale License	AG-0061
	Application for Tennessee Livestock Dealer License	AG-0064
	Livestock Market License Application	AG-0675
	Slaughter Swine Form	AG-0690
Apiary		
	Apiary Inspection Health Certificate	
	Apiary Inspection Request	
	Apiary Pest and Disease Specimen Form	
	Apiary Registration Form	
	Apiary Section Complaint Form	
	Application to Establish an Experimental Apiary in TN	
	Application to Move Honeybees or Used Equipment into TN	
	Customer Complaint Form	
	Honeybee Best Management Practices Agreement	
	Honeybee Best Management Practices Policy	
	Reporting Movement of Honeybee Colonies for Pollination within TN	
	Request for Apiary Information	
	Request to be Placed on List to Sell Local Honey and Other Products	
	Request to be Placed on Pollinator List for Growers	
	Request to be Placed on Structural Honeybee Removal List	
	Request to be Placed on Swarm Removal Services List	
	Request to be Removed From Any or All Above Lists	
Dairy Inspections - Applications		
	Application for Dairy Plant and/or Trade Products Plant License	
	Application for Distributors License	
	Application for Frozen Dessert Manufacture's License	D-5
	Application for Grade 'A' Milk Permit	
	Application for License Processing or Slaughtering of Meat and Poultry	
	Application for Registration of Dairy and-or Trade Products	AG-0354
	Application for Reinstatement of Permit	
	Application for Reinstatement of Sale of Product	

Section	Form	Form ID
	Application for Temporary Permit Status and Authorization for Civil Penalty Deduction	
	Application for Tennessee Egg License	
	Application for Tester's License	D-3
	Application for Vending Machine and Commissaries License	
	Sampler's/Weighmaster License Application	
Dairy - Inspection Reports (FDA) – Convert to TN Form		
	Bulk Milk Hauler-Sampler Evaluation Report	FDA 2399a
	Dairy Farm Inspection Report	FDA 2359a
	Manufacturing Plant Inspection Report – Single Service	FDA 2359c
	Milk Plant Equipment Test Report	FDA 2359b
	Milk Plant Inspection Report	FDA 2359
	Milk Sample Collector Evaluation Report - Dairy Plant Sampling - Raw and Pasteurized Milk	FDA 2399b
	Milk Tank Truck Inspection Report	
	Permission for Publication	FDA 2359o
	Report of Certification	FDA 2359d
Feed, Seed and Fertilizer		
	Annual Agricultural Liming Material Tonnage Report	
	Application for a Commercial Feed Facility License	
	Application for Seed License	AG-0308
	Application to Register Fertilizers	AG-0336
	Feed Tonnage Report	
	Grain Dealer License (Class 1 or 2)	AG-0627
	Incidental Grain Dealer	AG-0625
	License Application for Manufacturers of Commercial Lime	
	Public Grain Warehouse License	AG-0626
	Quarterly Fertilizer Tonnage Report	AG-0294
	Quarterly Report of Agricultural and Vegetable Seed Sold	AG-0687
Food and Dairy - Domestic Kitchen Permit		
	Domestic Kitchen Questionnaire	
	Sample Application Form	
Food and Dairy - Manufacturing Warehouse Permit		
	Plan Review Questionnaire	
	Sample Application Form	
Food and Dairy - Manufacturing Within Existing Establishment		
	Plan Review Questionnaire	
	Sample Application Form	
Food and Dairy - Other Permits		
	Sample Commercial Slaughter Application	
	Sample Egg License Application	
	Sample Vending Machine Application	
Food and Dairy - Retail Food Permit		
	Basic Requirements	
	Retail Request	
	Sample Application Form	
Food and Dairy - Retail Mobile Food Permit		

Section	Form	Form ID
	Farm Based Retail Meat Sales	
	Retail Plan Questionnaire	
	Sample Application Form	
Food and Dairy - Retail Mobile Seafood Permit		
	Retail Plan Questionnaire	
	Sample Application Form	
	Seafood Guidance	
Other Forms		
	Application - Registration of Farm Names	
Pesticides		
	Aerial Applicator Verification Form	AG-0137
	Additional Comments and Violations	AG-0609
	Application for Aerial Applicator License	
	Application for Duplicate or Replacement Certification Card	
	Application for Reciprocity in the State of Tennessee	
	Application for Restricted Use Pesticide Dealer License	
	Application for the Registration of Pesticides in Tennessee	
	Application to Take Certification Exam	
	Application to Take Commercial Pest Control License Exam	
	Apprentice Termite Technician School Registration Form - June	
	Apprentice Termite Technician School Registration Form - March	
	Apprentice Termite Technician School Registration Form - September	
	Certificate of Surety Bond for all other categories	AG-0105
	Certificate of Surety Bond for WDO, General Pest and Rodent, Bird, and Fumigation Structural	AG-0105
	Chain of Custody Report for Samples	AG-0583
	How to Complete the Product Registration Application	
	How to Obtain an Aerial Applicator License and Aircraft Decal	
	Marketplace Dealer Inspection Report	AG-0587
	Notice of Inspection	AG-0340
	Pest Control Applicator License and Charter (companies a-k)	
	Pest Control Applicator License and Charter (companies l-z)	
	Pesticide Application Inspection Report	AG-0586
	Pesticide Containment Checklist Report	
	Pesticide Investigation Request Form	AG-0568
	Pesticide Inspection Request Form	
	Pesticide Use Review Report	AG-0586
	Producer Establishment Inspection Report	
	Reciprocity Form for the State of Tennessee	
	Refillable Pesticide Container Checklist	
	Roster for Commercial Pesticide Applicator Recertification Point System in Tennessee	E&PP Info #81
	Sample Collection Report	
	South Carolina Non-refillable Pesticide Container Inspection	
	Statement	AG-0645
	Tennessee Pesticide Recertification - Application for Points	E&PP Info #82
	Termicide Calculation Sheet	

Section	Form	Form ID
	UT Pesticide Certification & Licensing Study Material Order Form	
	WPS Employee Interview	
	Worker Protection Use Inspection Report #1	AG-0554
	Worker Protection Use Inspection Report #2	AG-0556
Plant Certification		
	Application - Florist Certificate	
	Application - Greenhouse Certificate	
	Application - Hobbyist Greenhouse Certificate	
	Application - Hobbyist Nursery Certificate	
	Application - Landscaper Certificate	
	Application - Native Wild Plant	
	Application - Nursery Certificate	
	Application - Plant Dealer Certificate	
	Christmas Tree Inspection Report	
	Compliance Agreement – Cornus spp.	
	Compliance Agreement – Boxwood Blight	
	Compliance Agreement – Firewood	
	Compliance Agreement – Imported Fire Ant	
	Compliance Agreement – Japanese Beetle Harmonization	
	Compliance Agreement for Movement of Bare Root Stock into Oregon	
	Consumer Complaint Form	
	Emergency Action Notification	
	European Corn Borer Shipping Notification Permit	
	General Inspection Report	
	Greenhouse Inspection Report	AG-0100
	Hobbyist Greenhouse Certificate	AG-0592
	Hemp Movement Permit	
	Imported Fire Ant Monthly Report	
	Insect and Plant Disease Specimen Form - 1 eMail address	
	Insect and Plant Disease Specimen Form - 2 eMail addresses	
	Inspection Report	
	Native Wild Plant Inspection Report	AG-0099
	Nursery Inspection Report	AG-0100
	Permit for Movement	AG-338
	Plant Dealer Inspection Report	
	Shipping Quarantined Articles from European Corn Borer Infested Areas to Free Areas of Texas - Packer Shipper Agreement	
Time Management		
	Animal Health Version 5.1 111414	
Weights and Measures / Petroleum Quality		AG-0406
	Bulk Meter Test Report	AG-0220
	Certified Public Weigher License Application	
	Check Weighing & Price Verification Summary	
	Consumer Complaint	
	Grain Moisture Meter Report	
	Hopper Scale Test Report	P&SP-4500
	Official Notice of Equipment Rejection and/or Violation	AG-0225

Section	Form	Form ID
	Livestock Scale Test Report	P&SP-4200
	LPG Meter Examination	AG-0229
	Monorail Scale Test Report	P&SP-4300
	Petroleum Sample Collection Form	AG-0479
	Permit - Certified Public Weigher	
	Permit - Public Weight Master	
	Permit - Service Agency License	
	Permit - Service Person	
	Regulatory Services - Daily Time Log	AG-0581
	Random Pack Report	AG-0564
	Report of LPG Meter Examination	AG-0229
	Report of Price Verification System Inspection	AG-0558
	Report of Weighing Devices Tested	AG-0226
	Request for Inspection	
	Serviceperson Agency Application	AG-0178
	Serviceperson Application	
	Standard Pack Report	AG-0565
	Stop Sale Order and/or Seizure/Condemnation	AG-0483
	Terminal Meter Test Report	AG-0458
	Vehicle Scale Test Report	P&SP-4400
	W & M Device Fee Invoice	
	Weekly Summary and Itinerary	AG-0454
	Weighmaster License Application	AG-0193

Contractor Requirements

The Contractor will provide the Deliverables and meet the requirements specified in the Contract and its referenced attachments. The Contractor shall perform all of the activities and tasks required to achieve the objectives, functions, outputs, and performance criteria stated in the Contract. All services provided by the selected Contractor shall be appropriate and acceptable to the TDA project team and be consistent with State and Federal laws and regulations. The Contractor shall provide all of the staff necessary to perform the required services.

During the life of the project, the State will review Deliverables and evaluate them for completeness, clarity, adherence to generally recognized standards, and compliance with the contract. A Deliverable phase or milestone will not be considered complete until written approval has been given by the State. The process by which all Deliverables will be reviewed and accepted is outlined in Deliverable Acceptance.

The system will run in computing facilities maintained and operated by the Contractor. The State requires that the Contractor follow a systematic approach to the design, development, and implementation of the System to ensure that a comprehensive and expandable system is implemented. The State of Tennessee's Information Technology Methodology is Tennessee Business Solutions Methodology (TBSM). TBSM is based on the principles set forth by the Project Management Institute (PMI) and on industry best practices that are adapted to meet the state's needs. The contractor will be required to utilize these templates or templates comparable to the TBSM. The Contractor should address all the Deliverables for the life-cycle phases in their project plan but can organize and plan for the accomplishment of the work based on their experience with projects of similar scale and scope. The complete detailed requirements, which identify the required functionality of the System, are provided in Appendix 2 – *Functional and Technical Requirements*.

The contractor shall define the overall Project Management approach for the project and should describe, in general terms, the roles and authorities of project team members from both the State staff and the Contract staff. The Project Management Approach should be based on the Contractors best practices and experience, and should be fully described in the section of the Project Management Plan. The Contractor confirms their commitment to meet all requirements defined in this Appendix regardless of the approach proposed.

Each of the following subsections provides a narrative on the requirements, followed by a table defining the tasks and Deliverables to be fulfilled by the Contractor.

The Contractor shall provide project Deliverables for the system in the form and format agreed to by the State.

Project Initiation

The Project Initiation activity includes project planning for work performed for the TDA project contract. The complexity of the proposed System will require significant access and involvement of licensing Subject Matter Experts (SMEs).

During this activity, the project schedule will be developed, refined and confirmed, and risk assessment activities advance to the mitigation stage. The initial Project Schedule and Project Management Plans - are further developed, enhanced, and refined until they form a definitive plan for the rest of the project. The Contractor and the State will develop their project performance measures and collect the data to establish baseline performance. Contractor Deliverable or process requirements (CR) for the Project Initiation activities are described in Table 1.

Table 1, Project Initiation Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 1.	The Contractor shall identify the Project Management Approach which includes specific needs for information, materials, and decisions for TDA prior to the start of the Project Initiation phase of work proposed by the Contractor and request such information in writing. [See *Pro Forma* Contract Section A.3]	Project Management Approach
CR 2.	The Contractor shall refine and deliver its proposed project plans consistent with the resulting contract, including: • Project Scope Management Plan; • Milestone List; • Project Schedule Baseline; • Work Breakdown Structure (WBS); • Activity List; • Change Control Process; • Human Resource Plan; • Quality Management Plan; • Risk Management Plan; • Acceptance Management Plan; • Change Management Plan; • Issue Management and Escalation Plan; • Communication Management Plan; • Cost Management Plan; • Development, Implementation, and Transition Plans (including migration plans); • Requirements Development Plan; • Schedule Management Plan; • Performance Management Plan; • Training Plan; and • Fit/Gap Analysis	Project Plan
CR 3.	The Contractor shall refine the project schedule, including the project timeline, all major milestones, work breakdown structure, and a list of technical assumptions.	Project Schedule
CR 4.	The Contractor shall refine the project schedule, including defining the sequencing of project activities, the durations of the project activities, and any dependencies among the project activities for both the Contractor and State activities to create an agreed and approved project schedule baseline.	Master Project Schedule
CR 5.	The Contractor shall deliver the project schedule in MS Project format.	Project Schedule
CR 6.	The Contractor shall refine and deliver a project staffing plan that identifies individual resources (both State and Contractor resources) assigned to each of the project activities.	Staffing Plan
CR 7.	The Contractor should provide a Fit/Gap analysis. The analysis shall document, at a detailed level the extent to which the Proposer's software can meet the TDA required functions.	Requirements Verification and Fit/Gap
CR 8.	The Contractor shall describe the strategy that will be used to acquire human resources with the appropriate skills to staff the project.	Staffing Plan
CR 9.	The Contractor shall maintain job responsibility statements on file for all project personnel, including subcontractors and shall provide a copy to the State.	Human Resource Plan
CR 10.	The Contractor shall maintain and provide to the State an up-to-date organization chart and contact list providing name, title, phone, pager/cell phone, and email information for all Contractor personnel assigned to the project whenever Contractor personnel assignments change.	Human Resource Plan

Contractor Requirements		
	Task	**Deliverable or Process**
CR 11.	The Contractor shall refine and deliver a quality management plan that documents the quality standards and service level requirements of the project.	Quality Management Plan
CR 12.	The Contractor shall refine and deliver a quality management plan that documents all quality assurance activities to be implemented during the lifecycle of the project.	Quality Management Plan
CR 13.	The Contractor shall refine and deliver a risk management plan that shall include specific activities the Contractor will regularly perform to identify, qualify, quantify, prioritize, and manage risks.	Risk Management Plan
CR 14.	The Contractor shall refine and deliver a risk management plan that describes the actions to be taken to avoid, mitigate, or accept each risk impact.	Risk Management Plan
CR 15.	The Contractor shall refine and deliver a risk management plan that defines the frequency of risk management activities and status reporting.	Risk Management Plan
CR 16.	The Contractor shall work with the State to refine and deliver an acceptance management plan for the review and approval by the State of all project Deliverables including document-based Deliverables and software-based Deliverables.	Acceptance Management Plan
CR 17.	The Contractor shall refine and deliver a change management plan that describes the process for making any adjustment to any aspect of the project plan or to any already approved Deliverable(s). This includes anything formally documented in the project plan or any Deliverable produced during the course of the project.	Change Management Plan
CR 18.	The Contractor shall work with the State to refine and deliver a change management plan for the project that includes: • Identification of who is authorized to request a change; • Identification of who is responsible for analyzing the request's impact on the Project Cost, Scope, Schedule, and Quality; • Identification of who has authority to approve the request; • The timeframe (number of business days) allowed for a change request to be approved or rejected; • The process to follow if no timely decision on approval or rejection of a change request is made; and • The percentage of the overall Project Budget that has been reserved for project changes.	Change Management Plan
CR 19.	The Contractor shall refine and deliver an issue management plan for the project that includes: • How issues will be captured and tracked; • How issues will be prioritized; • How issues will be assigned; and • How and when issues will be escalated for resolution.	Issue Management and Escalation Plan
CR 20.	The Contractor shall refine and deliver a communications plan that describes how communications will be managed on the project, including: • How project information will be collected and stored, and what procedures will be followed to disseminate the information; • The distribution structure, specifically detailing what, how, and when information will flow to stakeholders; and • The method by which information will be accessed if it is needed between regularly scheduled communications.	Communications Plan

Contractor Requirements		
	Task	**Deliverable or Process**
CR 21.	The Contractor shall refine and deliver the project implementation and transition plans for implementing or deploying the System and for transitioning the responsibility of system operation from the Contractor to the State. This plan includes all the necessary activities to perform and procedures to follow to ensure a smooth and satisfactory hand-off.	Development, Implementation and Transition Plans
CR 22.	The Contractor shall refine and deliver the development, implementation, and transition plans, including: • A description of what needs to be done to ensure the State will be ready to receive the System; • An early assessment of agency readiness to allow mitigation of significant risks exposed by the assessment; • A description of how and when the Contractor recommends that the State will test and accept the System and confirm and authorize its implementation; • The steps to be taken to ensure that users will be ready to use the System once it is transitioned; • Recommended adjustments to the strategy for implementing the System (for example, phased by Participating Agency, specific license type(s), license function or other); • The steps that should be taken to ensure that the appropriate individuals are ready to support the System once it has been implemented and is in use; • Identification of the point in implementation at which the State takes responsibility for production problems, “help” or trouble calls, and for resolving the problems; • Identification of user and technical documentation to be delivered as part of the transition; and • Knowledge transfer approach describing how the State staff members will administer, maintain and support TDA without Contractor intervention.	Development, Implementation and Transition Plans
CR 23.	The Contractor shall refine and deliver a data conversion/data migration plan including: • A description of what the State needs to do to prepare existing data for import into the software database; and • How and when the State will test the validity and integrity of imported data.	Development, Implementation and Transition Plans
CR 24.	The Contractor shall provide a performance management plan that will include a detailed description of the methodologies, tools, and procedures in which the Contractor will manage and measure performance. The plan must also provide a listing of the items that will be measured, frequency of measurement, and appropriate metrics.	Performance Management Plan

Project Management

The Contractor shall designate a Project Manager to whom all communications may be addressed and who has the authority to act for the Contractor in all aspects of the services to be performed pursuant to this contract. The Project Manager will be responsible for directing the work of the Contractor’s staff. For a full description of how the State expects to govern and manage the project please refer to *Pro Forma* Contract A.3.

The Deliverable requirements for the project management activities are described in the table below:

Table 2, Project Management Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 25.	The Contractor shall update and implement the project quality management plan.	Quality Management Planning
CR 26.	The Contractor shall update and implement the risk management plan.	Risk Management Planning
CR 27.	The Contractor shall update and implement the project change control process.	Change Control Planning
CR 28.	The Contractor shall update and implement the project issue management and escalation process.	Issue Management Planning
CR 29.	The Contractor shall update and implement the project communication plan.	Communications Planning
CR 30.	The Contractor shall monitor the project for performance in accordance with baseline projections established within the contract deliverable dates. The Contractor Project Manager shall immediately advise the State Project Manager in writing, anytime it is determined the State Project team or the Contractors performance is jeopardizing the Project Work Plan, Project Scope, or the Project Budget. Any identified performance or delivery of critical path tasks/activities that could pose potential modification to the baseline work plan/schedule would be required to be presented to the Project Steering Committee and Change Control Board for review and approval.	All Phases/Project Schedule
CR 31.	The Contractor shall implement the project development, transition and implementation process.	Development, Transition and Implementation Management Planning
CR 32.	The Contractor shall attend all project meetings, including, but not limited to: • Kickoff Meeting – Within two weeks of final contract approval from the TDA, a kickoff meeting will be held at State offices to discuss start-up procedures; • Project Development Meetings – meetings related to project development and implementation as defined in the project communication plan and project schedule; • QA Meetings – quality assurance and review meetings as specified in the Contractor's Quality Assurance Plan; • Status Meetings – There shall be weekly project status meetings to review the progress and status of the tasks, problem areas, work to be accomplished, and other relevant items. Other ad hoc or periodic status meetings may be scheduled for specific communications needs; • Project Steering Committee Meetings – There shall be monthly Project Steering Committee meetings held at State offices to provide State staff and stakeholders with project status and accomplishments to date. The Contractor shall be responsible for preparing pre- and post-meeting documentation.	Communications Management Plan

Contractor Requirements		
	Task	**Deliverable or Process**
CR 33.	The Contractor shall provide status reports (periods to be determined by the State) to the State Project Team on the status of design and development metrics tasks, and milestones, including but not limited to: • Requirements status; • Design status; • Development status; • Test status; • Issue status; • Implementation status; and • Schedule status.	Communications Plan
CR 34.	Monthly Reporting Plan View - State requires a monthly status report for each project. The report is entered and updated in the State Project Portfolio Management tool, Plan view. Contractor will be responsible for providing required data elements for Plan view updates to this Project.	Communication Plan
CR 35.	Issue reports generated by the issue tracking system shall become part of Contractor's Status Reports.	Communications Plan
CR 36.	The Contractor shall provide the ability for initial issue creation and ongoing access/tracking of the issue tracking system to key State staff as designated by the State.	Issue Tracking System
CR 37.	The Contractor will develop a list of key performance measures and problem indicators jointly with State project management.	Performance Measures
CR 38.	The Contractor shall ensure that project Deliverables shall be subject to State review and approval prior to acceptance.	Acceptance Management Plan
CR 39.	The Contractor shall ensure that each project Deliverable is submitted to the State for review and acceptance with an approved deliverable specification sheet (to be developed jointly between the Contractor and the State after contract award).	Acceptance Management Plan
CR 40.	The Contractor shall ensure that each Deliverable shall address all components required by the contract including any areas identified subsequently through meetings and planning sessions, and the approved deliverable specification sheets.	Acceptance Management Plan
CR 41.	The Contractor shall certify in the cover letter for each Deliverable that the Contractor's internal deliverable review process was utilized.	Acceptance Management Plan
CR 42.	The Contractor shall ensure that for document-based Deliverables, the review and acceptance period reflects the time periods outlined in *Pro Forma* Contract A.10.a	Acceptance Management Plan
CR 43.	For Deliverables that contain hardware and/or software programs, the State's deliverable review process will incorporate acceptance testing as detailed in State approved Acceptance Test Plan.	Acceptance Management Plan
CR 44.	The Contractor shall ensure that, in the event the State agrees to accept, on an interim basis, a Deliverable with one or more sections left incomplete, the Deliverable shall include the date for completion, note the basis for the incomplete portions and the impact of any incomplete sections on project milestones.	Acceptance Management Plan
CR 45.	The Contractor shall identify in the project work plan the key documentation delivery milestones.	Project Schedule
CR 46.	The Contractor shall provide electronic copies of all documentation to the State in the format specified by the State, and supply hard copies as requested.	Development, Transition and Implementation Management Planning

Business Process Re-engineering

Business process re-engineering is required to develop the "To Be" in the TDA for the System. TDA have already invested considerable effort in documenting the current "As Is" business processes and will work with the Contractor to determine where improvements can be made.

Contractor Deliverable requirements for the business process re-engineering activities are described in the table below.

Table 3, Business Process Re-engineering Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 47.	The Contractor shall review existing "As Is" business process documentation, where it exists, and conduct a series of workshops with process stakeholders to confirm the "As Is" information and to ascertain changes that are required to complete the process documentation. Where "As Is" documentation does not exist, the Contractor shall conduct a series of workshops with process stakeholders to create the "As Is" business process documentation.	"As Is" Process Analysis
CR 48.	The Contractor shall review current business processes and develop an initial set of findings related to current processes. These findings will provide TDA with the rationale for the findings, the processes affected, the impact on the business function, and how improvement could positively affect the business function.	Review of Current Business Processes
CR 49.	The Contractor shall develop recommendations for process transformation based on the review of current processes. The Contractor shall document the areas for improvement identified and group the recommended business changes according to characteristics such as: changes to basic operating procedures; standardizing documentation; implementation of new technology; streamlining of current business processes; roles and responsibilities of organizational units; and changes to laws, policies, and regulations.	Recommendations for Process Transformation
CR 50.	The Contractor shall develop recommendations to address specific process improvement steps required by the business changes defined in the previous CR. The Contractor will provide short- and long-term process improvement recommendations based on this analysis. These recommendations will highlight specific procedural areas for improvement and demonstrate related improvement opportunities. For each recommendation, the Contractor shall identify: benefits to be gained; effect on process timeliness; estimated Return on Investment (ROI); impact on the organization; and re-defined process steps.	Recommendations for Process Transformation
CR 51.	The Contractor shall work with TDA to finalize and prioritize recommendations. Prioritization will be based on the potential benefits to be gained, timeframes in which to implement, ROI, process time efficiencies to be gained, and other environmental factors.	Recommendations for Process Transformation
CR 52.	The Contractor shall develop "To Be" process maps for each of the processes, depicting the new process with an analysis of the change in workflow.	"To Be" Process Maps
CR 53.	The Contractor shall develop an implementation plan that will serve as a roadmap for the TDA. This task will focus on the timeframe for implementation of changes to processes and procedures, and providing guidance on short- and long-term implementation depending on the nature of the recommendation.	BPI Implementation Plan

Organizational Change Management (OCM)

This OCM collaboration should also focus on reducing resistance and increasing speedy adoption and productivity during and after the implementation of the future state. This should include, at minimum, an end user Communication Plan, a Training Plan and a comprehensive Change Initiatives Plan. The expected outcome of the OCM Strategy is to reach ultimate productivity and business results as quickly as possible.

Table 4, Organizational Change Management

Contractor Requirements		
	Task	**Deliverable or Process**
CR 54.	The Contractor shall co-create, in conjunction with the State, an Organizational Change Management (OCM) Strategy. If the contractor does not already have knowledgeable OCM resources, the Contractors' Project Team will be working with an existing State OCM resource.	"Organizational Change Management Plan [assistance]

System Design

The purpose of System Design is to configure a technical solution that satisfies the functional requirements for the System. It is understood that a commercial software product has its own inherent design, so individual license/permit types will have to be retrofitted to that design, and/or customization of the software product may be undertaken to meet the State's requirements. As such, the Contractor, with TDA's assistance, will undertake a System Design effort that must occur for each license/permit type. This activity begins with a detailed review and analysis of the functional requirements to confirm a common understanding of how to evolve the requirements into the system design. The requirements are mapped to the enterprise architecture, and technical specifications are created for the implementation team, enabling them to configure and test the System. System Design is the time to initiate focused planning efforts for both the testing and data preparation activities. Test descriptions are to be developed, traced to requirements, and include the expected test results. Contractor requirements for the system design activities are described in Table 5 below.

Table 5, System Design Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 55.	The Contractor shall recommend specific methodologies for design and development activities prior to commencement of design or development activities for any customized components.	System Design Methodology
CR 56.	The Contractor shall work with the State on the completion of a detailed design of all license/permit types as defined in Appendix 2 – *Functional and Technical Requirements.*	Detailed Design Specifications
CR 57.	The Contractor shall develop and deliver a system architecture design document that describes the overall system architecture in terms of network, security, system, hardware, software, tools, peripherals, software licenses, and the logical distribution of system components and processes across the architecture.	System Architecture Design
CR 58.	During System Design, the Contractor shall deliver system security design documentation describing the logical security architecture design, the physical security architecture design, and the design of all controls to be used to mitigate threats to the confidentiality, integrity and availability of the System and system data.	System Security Design
CR 59.	The Contractor shall identify and document the database schemas, file formats, data views, an entity relationship diagram, and data dictionary for the System.	Database Documentation

Contractor Requirements		
	Task	**Deliverable or Process**
CR 60.	The Contractor shall deliver comprehensive data model documentation that clearly describes the conceptual, logical, and physical data characteristics of the System.	Data Model Documentation
CR 61.	The technical documentation shall include: • Anticipated data volume estimates; • Data needs for the system environment; • Updated data mapping; • Other interface descriptions; • Configuration report (that describes how each area of the licensing business is configured in the software); • Detailed specifications for hardware and software components; • System performance expectations; • Input on the State's cleansing and loading historical data as well as population of new data; and • Deployment plans.	Technical Documentation
CR 62.	The Contractor shall work with TDA to generate a detailed test plan defining: • The overall strategy for validating the functionality of the System; • The approach to ensure test coverage of each requirement; • The criteria for acceptance of each test; • The individual test cases that will be performed to execute the testing strategy; • The environments in which the tests will be conducted and data sources; and • The defect reporting and tracking tools for use by all agencies.	Test Plans
CR 63.	The test plans shall include: • Testing objectives; • Scope of testing (both what is in and what is out of scope); • Roles and responsibilities for test team members (who will be performing the test); • Testing approach; • Testing sequence; and • Defect reporting and criteria.	Test Plans
CR 64.	The test case descriptions shall be traced to requirements and include: • Test data needed to execute the tests; • Preconditions required prior to the start of test; • Criteria for suspending and resuming testing; and • Expected test results.	Test Plans

System Development

The System Development phase consists of all activities required to configure, customize, test, and validate the new system to the point at which it can be turned over for System Acceptance. This includes configuration and any required customization of all components of the System, including utilities required to adequately prepare and load the data. The Contractor will have to work with TDA to lay out a plan for developing and implementing the system. In addition, System Development consists of a series of tests of the system components, with each set of tests being performed against a progressively larger grouping of components until the full operation of the System has been verified. Actual test results will be documented and necessary corrective actions will be implemented in the System and system documentation. Status reports of testing progress will be provided on a regular basis

and will include the status of corrective actions. Since the ultimate goal of this activity is to produce a system that is ready for acceptance testing, an aspect of this phase is the creation of the various training materials and system documentation that support the new system, including preparation of help desk support and delivery of initial training. These materials need to address both the use and maintenance of the System and will play an integral part in the System Acceptance and System Implementation phases of the lifecycle. Deliverable requirements for the System Development activities are described in the table below.

Table 6, System Development Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 65.	The Contractor shall provide a system development methodology to support the software lifecycle that includes, but is not limited to, the use of commercially available system design and development tools.	System Development Methodology
CR 66.	The Contractor shall deliver a Requirements Traceability Matrix that identifies where and how each requirement has been addressed in the System.	Requirements Traceability Matrix
CR 67.	The Contractor shall utilize an industry standard testing methodology, to include unit testing, systems and integration testing, and user acceptance testing (functional, performance and reliability).	Test Methodology
CR 68.	The Contractor shall deliver test results including detailed outcomes for the following: • Data migration tests; • System tests (including performance tests); and • Security tests.	Test Results
CR 69.	The Contractor shall deliver test progress reports that include: • Number of defects identified in testing; • Types of defects found; and • Status of corrective actions.	Test Progress Reports
CR 70.	The Contractor shall update and deliver technical documentation to include corrective actions implemented as a result of testing activities.	Updated Technical Documentation
CR 71.	The Contractor shall update and deliver updated technical documentation including customization, system parameters, and configuration instructions.	Updated Technical Documentation
CR 72.	The Contractor shall develop and deliver the following user documentation that must be reflective of any specific configurations and customizations: • User Manual that will include instructions regarding the procedures the end-user would utilize to operate all modules of the System; • Database Administrator Manual, including installation and upgrade guides (this manual must address database refreshes); • System Administrator Manual; • System Operating Manual that will provide instructions regarding the phases, steps, and/or processes needed to operate the application and system software, including but not limited to application set up, user ID management, database maintenance and tuning, database and application recovery, and systems backup and recovery; • Frequently Asked Questions (FAQ) and scripts for help desk and technical support staff; • Documentation on how to incorporate customizations during system upgrades; and • Documentation on how to copy configuration and/or data to a new environment.	User Documentation
CR 73.	The user manuals shall include a collection of printable online documentation designed to instruct users in the operation of the System.	User Documentation

Contractor Requirements		
	Task	**Deliverable or Process**
CR 74.	The Contractor shall develop and deliver user training materials that provide instructions on the use of the System for all user roles, including any specific configurations and customizations.	Training Materials

System Acceptance

System Acceptance is the period in the project management lifecycle at which every aspect of the application being developed, along with any supporting data conversion routines and system utilities are thoroughly validated by TDA prior to proceeding with System Implementation. The System Acceptance phase is centered on gaining sufficient evidence of the System's accuracy and functionality to be able to proceed to System Implementation with the highest level of confidence possible in the success of the System. With the testing roadmap established in earlier lifecycle phases, the TDA will take responsibility for maneuvering the System through its operations. In addition to confirming the operation of the System and its fit to the business needs that it is intended to satisfy, System Acceptance is also the point in the lifecycle during which all supporting documentation and reference materials are refined and updated to guarantee their consistency with the final delivered system. Contractor Deliverable requirements for the System Acceptance activities are described in the table below.

Table 7, System Acceptance Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 75.	The Contractor shall deliver an updated Requirements Traceability Matrix that identifies where each requirement has been tested and the results of those tests.	Requirements Traceability Matrix
CR 76.	The Contractor shall deliver test results for the following: • Data validation results; • Data migration approach assistance • Acceptance test results (including performance tests); Security and vulnerability test results; and • Regression test results that re-test functions implemented in previous phases, to ensure the current phase implementation does not cause them to fail.	Test Results
CR 77.	The Contractor shall support acceptance testing to include both field testing for Point of Sale functions and user testing by the State.	Test Plans
CR 78.	The Contractor shall perform field testing for applicable staff TDA identifies for a time period of at least one month in an environment that has satisfactorily completed system/integration testing.	Test Plans
CR 79.	Acceptance of the System or system components will be contingent upon successful completion of acceptance testing as defined in any applicable Acceptance Test Plan as well as review and approval by the State of any other acceptance criteria as defined in the Acceptance Management Plan. The Contractor shall submit all project Deliverables through the acceptance management process developed and approved by the State during System Initiation.	Test Results
CR 80.	The Contractor shall identify the quality control (QC) measures and practices that will be implemented to ensure that the application is rigorously tested prior to implementation in production and is continuously monitored during the Project Period and System Warranty.	Test Plans

Contractor Requirements		
	Task	**Deliverable or Process**
CR 81.	The Contractor shall provide comprehensive performance testing, prior to cutover, that demonstrates the processing and response times of critical functions and transactions under various operational conditions (e.g., scenario scripts and system load and stress).	Test Results
CR 82.	The Contractor shall compile test data and provide test results within the time period specified in the Test Plan.	Test Results
CR 83.	The Contractor shall license testing tools for use by the State.	Testing Tools
CR 84.	The Contractor shall provide a classification and tracking method for system or application errors during acceptance testing that describes the severity of deficiency, and determination, based upon severity, of whether that error must be corrected prior to User Acceptance.	Issue Tracking System
CR 85.	The Contractor shall deliver an accepted system.	Accepted System
CR 86.	The Contractor shall deliver accepted migrated data in the System.	Migrated Data
CR 87.	The Contractor shall refine and deliver the following user documentation: • User Manual; • Database Administrator Manual, including installation and upgrade guides; • System Administrator Manual; • System Support Plan describing how to maintain the system configurations and customizations; • FAQs and scripts for help desk and technical support staff; • Documentation on how to incorporate customizations during system upgrades; and • Guide to standard reports.	Updated Technical Documentation
CR 88.	The Contractor shall deliver system security documentation describing the logical security architecture, the physical security architecture, and all controls that are used to mitigate threats to the confidentiality, integrity, and availability of the System and system data.	System Security Documentation
CR 89.	The Contractor shall refine and deliver training materials for all user roles.	Training Materials

System Implementation

The purpose of System Implementation can be summarized as the deployment and the transition of system support responsibilities. At a finer level of detail, deploying the System consists of executing all steps necessary to educate the system users on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the System are functioning properly. Deliverable requirements for the System Implementation activities are described in the table below.

Table 8, System Implementation Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 90.	The Contractor shall deliver an operational system to the TDA that fulfills all system requirements.	Operational System
CR 91.	The Contractor shall deliver approved installation and data migration scripts to the TDA to promote the System to the appropriate database environments.	Data Migration Scripts
CR 92.	The Contractor shall take into account available windows of opportunity (due to annual processes and ongoing business operations) when determining the deployment timing of various functionality.	Installation and Deployment

Contractor Requirements		
	Task	**Deliverable or Process**
CR 93.	The Contractor must allow for flexible enforcement of the business rules during the implementation year where there will be item sales in both the current and new automated sales environments.	Installation and Deployment
CR 94.	Following the implementation of any system phase or component, the State, with assistance from the Contractor, shall monitor the production system to verify performance in accordance with all requirements and acceptance criteria for a period set forth in the Acceptance Management Plan and any applicable Acceptance Test Plans. Such monitoring will be conducted on-site and the Contractor shall provide all necessary resources to correct any defects promptly according to Service Levels identified in the *Pro Forma* Contract, Section A.67 – Support.	Production Verification Testing
CR 95.	The Contractor shall provide documentation and training to support the process of defect tracking and corrective action.	Issue Tracking Documentation
CR 96.	The Contractor shall be responsive to State staff operating the State's Help Desk when access to system support or technical assistance is requested or required.	Support for State Help Desk
CR 97.	The Contractor shall implement the System in the production environment in accordance with the approved Project Implementation and Transition Plan.	Implementation and Transition Assistance
CR 98.	The Contractor shall conduct knowledge transfer in accordance with the approved project knowledge transfer approach.	Knowledge Transfer
CR 99.	The Contractor shall provide the TDA with the software release schedule for the software components contained within the System.	Software Release Schedule

Training Requirements

The proposed system will be a complex system that will be used daily by TDA staff. The State considers the training of these users to be critical for acceptance of the System as well as the daily use of the System. The System project team will review and approve all Contractor System training staff and user training materials, including training plans and role-based training materials.

The project team training responsibilities include:

- Review and approval of all role-based System training schedules.
- Review and approval of all Contractor training staff.
- Review and approval of the overall System training plan.
- Identify all staff to be trained during the implementation by role.
- Review and approval of all Contractor-developed role-based System training materials.
- Provide training facilities, computers, and network connections for all of the System training sessions.
- Designate a training environment for use during training.
- Coordinate training activities with the State's Learning Management System as appropriate.

The TDA Staff Training Requirements are described in the table below.

Table 9, TDA Staff Training Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 100.	The Contractor shall provide all training materials (to include training curriculum/syllabus, training objectives etc.) for the training sessions.	Training Materials

Contractor Requirements		
	Task	**Deliverable or Process**
CR 101.	The Contractor shall provide training materials (in electronic format in a form acceptable to the State) to the State for approval at least 15 days prior to the training.	Training Materials
CR 102.	Training sessions will occur at least 30-60 days before the system implementation.	Training Sessions
CR 103.	The Contractor shall provide assistance to the TDA to implement a training environment in the designated technical environments.	Training Database
CR 104.	The Contractor shall provide the capability to refresh the System training environment for each training session.	Training Database
CR 105.	The Contractor shall develop the training data based on Participating Agency input and/or migrated/converted data.	Training Database
CR 106.	The Contractor shall provide training session attendance records to TDA.	Training Attendance Records
CR 107.	The Contractor shall provide web-based ad hoc training for self-study users.	Web-based Training
CR 108.	The Contractor shall perform a training needs analysis that identifies: • Critical training focus areas; • Role-based training modules; and • Role-based training media.	Training Needs Analysis
CR 109.	The Contractor shall refine and deliver a training plan identifying: • Schedule for all role-based training sessions; • Training evaluation collection, analysis, and improvement process; • Success metrics identification, collection, and evaluation process; • Expected training results; and • Post Training Support.	Training Plan
CR 110.	The Contractor shall develop customized TDA project role-based training for each role. Role-based training materials may include: • Participant Guidebooks (Printed [defined number by TDA] and Electronic) including exercises; • Instructor Guidebooks (Printed and Electronic) including exercises and answers; • PowerPoint Presentations; • User Manuals; and • Online Help.	Training Materials
CR 111.	The Contractor shall develop step-by-step instructions for adding a new license/permit type that will allow State staff to implement new license types without Contractor assistance.	Instructions for adding license types
CR 112.	The Contractor shall plan, organize, staff, direct, and control the training and development activities to meet the organizational and training goals of the project.	Training Sessions
CR 113.	The Contractor shall manage the training program, report all activities, and schedule all activities.	Training Sessions
CR 114.	The Contractor shall plan and perform training sessions in the TDA training locations indicated in the Staff Training Estimates table (Table 5). The Contractor will provide any specialized computer equipment (i.e. equipment other than a PC, projector or printer).	Training Sessions
CR 115.	The Contractor shall provide approved training staff for each System training session.	Training Session Staff
CR 116.	The Contractor shall coordinate with the TDA to schedule the role-based training prior to system implementation.	Role Based Training Sessions
CR 117.	The Contractor shall update all System training schedules to address any State comments.	Training Sessions

Contractor Requirements		
	Task	**Deliverable or Process**
CR 118.	The Contractor shall provide a mechanism for collecting training session evaluations (e.g. web-based survey tool)	Training Materials
CR 119.	The Contractor shall provide coaching and mentoring support for training session attendees for the implementation.	Coaching and Mentoring Support
CR 120.	The Contractor shall develop FAQ to document coaching requests and the provided responses to participating System users	Coaching and Mentoring Support
CR 121.	The Contractor shall update training material to clarify areas where repetitive coaching questions are received.	Training Materials
CR 122.	The Contractor shall develop Help Desk Diagnostic Scripts to aid Help Desk Personnel in diagnosing problems.	Diagnostic Scripts
CR 123.	The Contractor shall provide mentoring scripts for the Help Desk to follow in order to provide mentoring support after the Contractor mentoring support ends.	Mentoring Scripts
CR 124.	During Implementation, the Contractor shall coach and mentor TDA staff, enabling their ability to support and maintain the System.	Coaching and Mentoring Support
CR 125.	The Contractor shall update impacted training material whenever software changes, including customizations, affect the operation of the software.	Training Materials
CR 126.	The Contractor shall provide technical training for staff who will take over the administration of the System once in production. The Contractor shall provide training to State technical staff, including but not limited to: • Database structure and design; • System and application architecture; • Query development; and • Report development.	Technical Training Sessions
CR 127.	The Contractor shall provide training to State test staff on the testing procedures outlined in Section A.17 - Training Requirement.	Test Procedure Training Sessions
CR 128.	The Contractor will provide TDA a “Train-the-Trainer” approach that will allow key State staff to acquire the knowledge of the System necessary to be able to deliver End-user Training.	Train the Trainer Approach & Materials

The table below presents estimates of the numbers of users that will need to receive in depth training on the use or administration of the System.

Table 10, TDA Staff Training Estimates

Training Locations

Level	Training Description	Training Location	Maximum Number of Attendees
1	System Administrator Training	Nashville, TN – TDA Office	Maximum of 4
2	Account Administrator Training	Nashville, TN – TDA Office	Maximum of 4
3	Train the Trainer	Nashville, TN – TDA Office	Maximum of 10
4	General End User Training	Initial training shall be conducted in Nashville, TN.	Maximum of 20

Table 11, Maintenance and Support

Contractor Requirements		
	Task	**Deliverable or Process**
CR 129.	The software provider shall provide a System Support Plan that documents the detailed support procedures, including request initiation, prioritization, problem resolution, escalation, tool usage, organization and individual roles and responsibilities, and reporting requirements.	Maintenance & Support
CR 130.	The software provider shall provide Maintenance and Support in accordance with the Maintenance and Support Plan that results from this procurement, with services beginning immediately following the System Warranty period. At a minimum, the Maintenance and Support agreement will address the following: • Software issue resolution; • Access to Contractor Issue Tracking System for the State System support team; • Service Levels; • Software upgrades; • Technical assistance for the State System support team in the installation and regression testing of software upgrades; • Updates to user, technical, and training documentation to support software changes resulting from fixes or upgrades; • Remote diagnostics; and • On-site issue resolution if necessary.	Maintenance & Support
CR 131.	The software provider shall provide software maintenance and support for TDA staff members in accordance with agreed upon Service Levels.	Maintenance & Support
CR 132.	The software provider shall attend software support status meetings with TDA personnel as needed.	Maintenance & Support
CR 133.	The software provider shall provide recommendations on upgrading to new releases of the Software.	Maintenance & Support
CR 134.	The software provider shall maintain a software upgrade plan that will handle system customizations with minimal effort required by the State.	Maintenance & Support
CR 135.	The software provider shall prepare a rollback plan, mutually agreed to by the State, prior to any migration of any new releases of the Software or patches to the Software to the production environment.	Maintenance & Support
CR 136.	The software provider shall advise the State in writing within ten (10) days of notice from the State of a proposal to change software used in conjunction with the System, or at such later date as agreed to by the State.	Maintenance & Support
CR 137.	The software provider shall advise the State in writing whether the proposed replacement software is compatible with the System so that the System shall continue to operate at the same (or higher) level of performance as was achieved at the time of Final Acceptance. In the event the software provider advises the State that the proposed replacement software does not satisfy the requirements set forth here, the software provider shall, in its response to the State, recommend alternatives to the proposed replacement software, and, if necessary, modifications to the existing software and system that will satisfy such requirements. Examples of software that the State may change include, but are not limited to the database, operating system, web browser, or word processor.	Maintenance & Support

Table 12, System Support and System Warranty

Contractor Requirements		
	Task	**Deliverable or Process**
CR 138.	The Contractor shall provide a System Support Plan that documents the detailed support procedures, including request initiation, prioritization, problem resolution, escalation, tool usage, organization and individual roles and responsibilities, and reporting requirements.	System Support Plan
CR 139.	The Contractor shall provide System Support beginning at the first Implementation Stage through the Retainage Period. At a minimum, the System support plan will address the following: • Software issue resolution; • Access to Contractor Issue Tracking System for the System support team; • Service Levels; • Software upgrades; • Installation and regression testing of software upgrades; • Updates to user, technical, and training documentation to support software changes resulting from fixes or upgrades; • Remote diagnostics; and • On-site issue resolution if necessary.	System Support & System Warranty
CR 140.	Commencing from User Acceptance of the first Implementation Stage through the Retainage Period, the Contractor shall warrant the following: • Components or Deliverables specified and furnished by or through the Contractor in the course of providing the services described in the Agreement shall, individually and together, operate in accordance with all Acceptance Criteria for such Deliverables and the System and shall operate substantially uninterrupted and error-free, and be guaranteed against faulty material and workmanship. • Defects in the materials or workmanship of components or Deliverables specified and furnished by or through Contractor shall be promptly repaired or replaced by Contractor at no cost or expense to the State. • Accepted Deliverables and the System as a whole shall (i) continue to meet the functional, performance and reliability requirements of the State, as set forth in the RFQ and the resulting Agreement and the manufacturers' specifications for the Equipment and Software, as the same may be amended and updated and (ii) operate in conformance with the acceptance criteria established for each Deliverable, the System as a whole, and by the Acceptance Management Plan.	System Support & System Warranty
CR 141.	Commencing from User Acceptance of the first Implementation Stage through the Retainage Period, the Contractor shall promptly provide all necessary services and support at no cost to the State to ensure all Deliverables and the System operate in accordance with the warranties set forth in Table 11 above.	System Support & System Warranty
CR 142.	Commencing upon the completion of the Retainage Period, the system shall enter the Warranty phase, as defined in the *Pro Forma* Contract, Section A.18.	System Support & System Warranty

Contractor Requirements		
	Task	**Deliverable or Process**
CR 143.	Where the Contractor or other third-party manufacturer / developer markets any project Deliverable delivered by or through Contractor with a standard commercial warranty, such standard warranty shall be in addition to, and not relieve the Contractor from, the Contractor's obligations for System Support described herein. Where such standard commercial warranty covers all or some of the Project Period, Contractor shall be responsible for the coordination with other third-party Product manufacturer(s) / developer(s) for warranty repair or replacement of other third-party manufacturer's / developer's Product.	System Support & System Warranty
CR 144.	Where the Contractor or other third-party Product manufacturer(s) / developer(s) market any Project Deliverable with a standard commercial warranty which goes beyond the Project Period, the Contractor shall notify the State and pass through the manufacturer's standard commercial warranty to the State at no additional charge.	System Support & System Warranty
CR 145.	The Contractor shall provide the TDA staff members with access to a bug-reporting and enhancement-tracking system.	System Support & System Warranty
CR 146.	The Contractor shall provide technical and application support for TDA staff members in accordance with agreed upon Service Levels.	System Support & System Warranty
CR 147.	The Contractor shall attend software support status meetings with TDA personnel as needed.	System Support & System Warranty
CR 148.	The Contractor shall provide recommendations on upgrading to new releases of the Software.	System Support & System Warranty
CR 149.	The Contractor shall devise a software upgrade plan that will handle TDA customizations with minimal effort required by the State.	System Support & System Warranty
CR 150.	The Contractor shall prepare a rollback plan, mutually agreed to by the State, prior to any migration of any new releases of the Software or patches to the Software to the production environment.	System Support & System Warranty
CR 151.	The Contractor shall advise the State in writing within ten (10) days' notice of a proposal to change software used in conjunction with the System, or at such later date as agreed to by the State. The software provider shall advise the State in writing whether the proposed replacement software is compatible with the System so that the System shall operate in conformance with the Acceptance Criteria for the System. In the event the software provider advises the State that the proposed replacement software does not satisfy the requirements set forth there, the software provider shall, in its response to the State, recommend alternatives to the proposed replacement software, and, if necessary, modifications to the existing software and system that will satisfy such requirements. Examples of software that the State may change include, but are not limited to the database, operating system, web browser, or word processor.	System Support & System Warranty
CR 152.	The State seeks a System Warranty as described in this section; the Contractor will continue to provide the same level of support as during the Project Period for the System during an anticipated twelve month period following the Final Acceptance of the System.	System Warranty

The State's Acceptable Use Policy and Acceptance Use Agreement begins on next page.

STATE OF TENNESSEE

Administrative User Policy
Network, Data and Information Resource Access Rights and Obligations

Purpose
To ensure that individuals who are in a position of trust and/or operate information systems with elevated privileges understand his/her rights, responsibilities, obligations and consequences of misuse.

References:
Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994.
Tennessee Code Annotated, Section 10-7-504, effective July 1, 2001.
State of Tennessee Security Policies.

Objectives:
- Ensure the protection of proprietary, confidential, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
- Ensure that individuals who are granted escalated system and/or network resource privileges do not abuse such privileges for personal gain.
- Ensure that individuals do not take actions that result in obtaining money, knowledge, property, or an advantage to which those individuals are not entitled.
- Ensure that individuals do not intentionally, wrongfully, or improperly use or destroy State information resources, or conduct improper practices not limited to prosecutable fraud.
- Maintain security of and access to networked data and information resources on an authorized and trusted basis.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users granted administrative and/or privileged rights of his/her network access rights and obligations.

Scope
This Administrative User Policy applies to all individuals who have been provided administrative access rights to the State of Tennessee networks, State provided email, and/or Internet via agency issued network or system User ID's or physical access to such resources. The scope does not include State phone systems, fax machines, copiers, State issued cell phones or pagers unless those services are delivered over the State's IP network.

Network, Data and Information Resources Usage
State employees, vendors, business partners or subrecipients, local governments, and other governmental agencies may be authorized to access state network, data or information resources to perform business functions with or on behalf of the State. Users granted administrative rights must be acting within the scope of his/her employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature.

Network, Data and Information Resources Prohibitions

- Accessing, viewing, copying, sending, sharing and/or selling any information that is confidential by law, rule or regulation, or not otherwise available, without proper authorization.
- Leaving workstation(s) unattended without logging off or engaging password protection for the privileged account for which the user is responsible.
- Utilizing unauthorized, unlicensed, hacked, cracked or stolen software on computing platforms which could subject privileged accounts to further risk.
- Using network, data or information resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing network, data or information resources for activities that violate conduct policies established by the Information Systems Council (ISC), the Department of Human Resources, The Department of Finance and Administration, the Office for Information Resources and/or the Agency where the user is employed or under contract.
- Using escalated privileges to remove audit trails, system log files and/or security event logs in an effort to hide any data that would provide evidence supporting a violation of this policy.

Statement of Consequences

Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's information technology operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Statement of Enforcement

Noncompliance with this policy may result in the following actions:

1. Written notification will be sent to the Agency Head and to designated points of contact in the User Agency's Human Resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance issue. In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
2. Administrator user access credentials may be terminated immediately, and the individual may be subject to subsequent review. These actions may be grounds for disciplinary action up to and including dismissal as determined by the Agency Head.

STATE OF TENNESSEE

Administrator User Policy
Network, Data and Information Resource Access Rights and Obligations
User Agreement Acknowledgement

As an administrative or privileged user of State of Tennessee network, data or information resources, I agree to abide by the Administrator User Network, Data and Information Resource Access Rights and Obligations Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State confidential data, facilities and systems entrusted to me against unauthorized disclosure and/or use.
2. I will maintain all network, data and/or computer access credentials assigned to me in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
3. I will be accountable for all transactions performed using my computer access credentials.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.
5. I have read and agree to abide by the Data Center Processing Physical Security Policies that are in effect on the data of my signature below.
6. I agree to report any suspicious network, data and/or computer activity, security breach or violation of this policy to my supervisor.
7. Upon the termination of my employment or contractual relationship with the State of Tennessee, I will not disclose any proprietary, confidential, privileged, or otherwise sensitive data and resources.

Privacy Expectations
The State of Tennessee actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. These communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving administrative and/or privileged access to State of Tennessee data and information resources.

I understand the willful violation or disregard of any of these guidelines, statute or policies may result in my loss of access and disciplinary action, up to and including my dismissal, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Tennessee Personal and Commercial Computer Act of 2003 as cited at TCA 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

_____	_____
Type or Print Name	Edison ID
_____	_____
Signature	Date

REQUEST FOR CONFIDENTIAL DOCUMENTS

In order to receive the confidential documents described in Section 1.4 of the RFP, the State must receive a Notice of Intent to Propose (filed separately) and a signature on the attached Confidentiality Agreement by an officer of the prospective respondent who is authorized to bind the company.

NON-DISCLOSURE AGREEMENT (NDA)

_____, a Prospective Respondent on a procurement with the State of Tennessee (hereinafter "Prospective Respondent"), will be provided with copies of the following documents for the purposes of preparing a response to this procurement.

1. Edison Business Partner Interfaces – Technical Quick Start Guide

2. Enterprise Technology Architecture Standard Products

In consideration for access to these documents, Prospective Respondent agrees as follows:

1. These documents are confidential and proprietary and are not public records of the State of Tennessee.

2. These documents, or copies thereof, will only be disclosed to authorized employees and contractors of Prospective Respondent who need access to them for the purpose of preparing a response to the procurement. All individuals entrusted with these documents, or the information contained therein, will be notified of the confidentiality restrictions.

3. Prospective Respondent will maintain reasonable security procedures to protect paper and electronic copies of these documents.

4. If Prospective Respondent chooses not to offer a response or if the response does not result in a contract with the State, the Prospective Respondent will destroy all copies of the documents within a reasonable time. If requested by the State, Prospective Respondent will certify in writing that the confidential documents were destroyed.

5. If Prospective Respondent enters into a contract with the State based on this procurement, this confidentiality agreement will expire upon signature of the contract, and the confidentiality provisions of the contract will control.

6. Prospective Respondent agrees that unauthorized release of the documents would cause such harm to the State that injunctive relief would be an appropriate remedy. If any court rules that Prospective Respondent has breached this confidentiality agreement, Prospective Respondent shall reimburse the State for its cost of litigation, including attorney's fees, as well as any damages awarded by the court.

7. This confidentiality agreement shall be interpreted under the laws of the State of Tennessee.

_____
(signature)

_____
(name of company)

Signature of this document constitutes certification that the person signing the document has the authority to bind the company.

_____

for State of Tennessee

The *Public Enterprise Information Security Policies – v2.0* begins on next page.

Enterprise Information Security Policies

State of Tennessee
Department of Finance and Administration
Office for Information Resources
Information Security Program

Document Version 2.0 – December 22, 2014

Table of Contents

		Page
1.	EXECUTIVE SUMMARY	1
2.	INTRODUCTION	3
	Scope (2.1)	4
	Authority (2.2)	4
	Exceptions (2.3)	5
	Review (2.4)	5
	Document Format (2.5)	5
	Policy Maintenance (2.6)	6
3.	INFORMATION SECURITY POLICIES	7
	Management Direction for Information Security (3.1)	7
	Policies for Information Security (3.1.1)	7
	Policies for Information Security (3.1.2)	7
	Policies for Information Security (3.1.3)	7
4.	OPERATIONS SECURITY	8
	Operational Procedures and Responsibilities (4.1)	8
	Documented Operating Procedures (4.1.1)	8
	Change Management (4.1.2)	8
	Change Control Procedures (4.1.2.1)	8
	Capacity Management (4.1.3)	8
	Separation of Development, Testing and Operational Environments (4.1.4)	8
	Protection from Malware (4.2)	9
	Malicious Software Control (4.2.1)	9
	Backup (4.3)	9
	Data Backup (4.3.1)	9
	Logging and Monitoring 4.4)	9
	Event Logging (4.4.1)	9
	Availability and Performance Monitoring (4.4.2)	10
	Protection of Log Information (4.4.3)	10
	Administrator and Logs (4.4.4)	10
	Clock Synchronization (4.4.5)	10
	Control of Operational Software (4.5)	10
	Installation of Software on Operational Systems (4.5.1)	10
	Patch Management (4.5.1.1)	10
	Software Development Code (4.5.1.2)	11
	Review of Application and Operating System Changes (4.5.1.3)	11
	Technical and Vulnerability Management (4.6)	11
	Management of Technical Vulnerabilities (4.6.1)	11
	Restrictions on Software Installation (4.6.2)	11
	Information Systems Audit Considerations (4.7)	11
	Information Systems Audit Controls (4.7.1)	11

5. ACCESS CONTROL 12

Business Requirements of Access Control (5.1) 12
Access Control Policy (5.1.1) 12
Access to Networks and Network Services (5.1.2) 12
Remote Access (5.1.2.1) 12
Information Security Roles and Responsibilities (5.1.3) 12
Segregation of Duties (5.1.4) 12
User Access Management (5.2) 13
User Registration and De-Registration (5.2.1) 13
User Access Provisioning (5.2.2) 13
User Account Naming (5.2.2.1) 13
Management of Privileged Access Rights (5.2.3) 13
Management of Secret Authentication of Information Users (5.2.4) 13
Review of User Access Rights (5.2.5) 13
Removal or Adjustment of Access Rights (5.2.6) 14
User Responsibilities (5.3) 14
Use of Secret Authentication Information (5.3.1) 14
System and Application Access Control (5.4) 14
Information Access Restriction (5.4.1) 14
Secure Log-on Procedures (5.4.2) 14
System Administrator Access (5.4.2.1) 14
Logon Banner (5.4.2.2) 14
Service Account Use (5.4.2.3) 15
Password Management System (5.4.3) 15
Use of Privileged Utility Programs (5.4.4) 15
Access Control to Program Source Code (5.4.5) 15
Default Configurations (5.4.6) 15

6. ASSET MANAGEMENT 16

Responsibility for Assets (6.1) 16
Inventory of Assets (6.1.1) 16
Ownership of Assets (6.1.2) 16
Acceptable Use of Assets (6.1.3) 16
Return of Assets (6.1.4) 16
Asset Identification (6.1.5) 16
Data Classification (6.2) 16
Classification of Data (6.2.1) 17
Labelling of Data (6.2.2) 17
Handling and Use of Data (6.2.3) 17
Public Data Classification and Control (6.2.3.1) 17
Confidential Data Classification and Control (6.2.3.3) 17
Confidential Data on Personally Owned Devices (6.2.3.4) 17
Confidential Electronic Messages Classification and Control (6.2.3.5) 18
Payment Card Information Classification and Control (6.2.3.6) 18
Use of Confidential Data (6.2.3.7) 18
Media Handling (6.3) 19
Management of Removable Media (6.3.1) 19

Repair of Removable Media (6.3.1.1) 19
Disposal of Removable Media (6.3.2) 19
Physical Transfer of Removable Media (6.3.3) 19
Workstation Computing (6.4) 19
State Provided Workstation Computing Platforms (6.4.1) 19
Workstation Platform Reassignment (6.4.2) 20
Workstation Platform Disposal (6.4.3) 20
Cloud Services (6.4.4) 20

7. PHYSICAL AND ENVIRONMENTAL SECURITY 21

Secure Areas (7.1) 21
Physical Security Perimeter (7.1.1) 21
Physical Entry Controls (7.1.2) 21
Securing Offices, Rooms and Facilities (7.1.3) 21
Protecting against External and Environmental Threats (7.1.4) 21
Working in Secure Areas (7.1.5) 21
Delivery and Loading Areas (7.1.6) 21
Equipment (7.2) 22
Equipment Siting and Protection (7.2.1) 22
Supporting Utilities (7.2.2) 22
Cabling Security (7.2.3) 22
Equipment Maintenance (7.2.4) 22
Removal of Assets (7.2.5) 22
Security of Equipment and Assets Off-Premises (7.2.6) 22
Secure Disposal or Re-Use of Data Processing Equipment (7.2.7) 23
Unattended User Equipment (7.2.8) 23
Session Time Outs (7.2.8.1) 23
Clear Desk and Clear Screen Policy (7.2.9) 23

8. NETWORK CONNECTIVITY SECURITY 24

Network Security Management (8.1) 24
Network Controls (8.1.1) 24
Security of Network Services (8.1.2) 24
Segregation in Networks (8.1.3) 24
Information Transfer (8.2) 24
Information Transfer Policies and Procedures (8.2.1) 24
Agreements on Data Transfer Policies (8.2.2) 24
Electronic Messaging (8.2.3) 25
Internal Electronic Messages Control (8.2.3.1) 25
External Electronic Messages Control (8.2.3.2) 25
Electronic Messaging Management (8.2.3.3) 25
Confidentiality or Non-Disclosure Agreements (8.2.4) 25

9. MOBILE DEVICE SECURITY POLICY 26

Mobile Devices and Teleworking (9.1) 26
Mobile Device Policy (9.1.1) 26
Teleworking (9.1.2) 26

10. EXTERNAL PARTY SECURITY 27

Information Security for External Party Relationships (10.1) 27
Information Security Policy for External Party Relationships (10.1.1) 27
Identification of Risk (10.1.2) 27
Addressing Security within External Party Agreements (10.1.3) 27
Reporting of Security Incidents (10.1.3.1) 27
Sub-Contractors Requirements (10.1.3.2) 27
Addressing Security for Access to Citizen Data (10.1.4) 28

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE 29

Security Requirements of Information Systems (11.1) 29
Security Requirements of Information Systems (11.1.1) 29
Securing Application Services on Public Networks (11.1.2) 29
Protecting Application Services Transactions (11.1.3) 29
Information Security in Project Management (11.1.4) 29
Security in Development and Support Processes (11.2) 29
Security Requirements of Information Systems (11.2.1) 29
Security in Application Systems Development (11.2.1.1) 30
Input and Data Validation (11.2.1.2) 30
Output Data Validation (11.2.1.3) 30
Application Authorization (11.2.1.4) 30
Inter-process Message Authentication (11.2.1.5) 30
Control of Internal Processing (11.2.1.6) 30
System Change Control Procedures (11.2.2) 30
Technical Review of Applications after Operating Platform Changes (11.2.3) 30
Restrictions or Changes to Software Packages (11.2.4) 31
Secure System Engineering Principles (11.2.5) 31
Secure Development Environment (11.2.6) 31
Outsourced Development (11.2.7) 31
System Security Testing (11.2.8) 31
System Acceptance Testing (11.2.9) 31
Test Data (11.3) 31
Protection of Test Data (11.3.1) 31

12. BUSINESS CONTINUITY MANAGEMENT 32

Information Business Continuity (12.1) 32
Planning Information Systems Continuity (12.1.1) 32
Business Impact Analysis (12.1.1.1) 32
Critical Applications (12.1.1.2) 32
Non-Critical Applications (12.1.1.3) 32
Implementing Information Systems Continuity (12.1.2) 32
Verify, Review and Evaluate information Systems Continuity (12.1.3) 33
Redundancies (12.2) 33
Availability of Information Processing Facilities (12.2.1) 33

13. INFORMATION SECURITY INCIDENT MANAGEMENT 34

Management of Information Security Incidents and Improvements (13.1) 34
Responsibilities and Procedures (13.1.1) 34
Reporting Information Security Events (13.1.2) 34
Data Breach and Disclosure (13.1.2.1) 34
Reporting Information Security Weakness (13.1.3) 35
Assessment of and Decision on Information Security Events (13.1.4) 35
Response to Information Security Incidents (13.1.5) 35
Learning from Information Security Incidents (13.1.6) 35
Collection of Evidence (13.1.7) 35

14. CRYPTOGRAPHY 36

Cryptographic Controls (14.1) 36
Use of Cryptographic Controls (14.1.1) 36
Transmission Integrity (14.1.2) 36
Transmission Confidentiality (14.1.3) 36
Cryptographic Module Authentication (14.1.4) 36
Cryptographic Module Authentication (14.1.5) 37
Key Management (14.1.6) 37

15. COMPLIANCE 38

Compliance with Legal and Contractual Requirements (15.1) 38
Identification of Applicable Legislation and Contractual Requirements (15.1.1) 38
Intellectual Property Rights (15.1.2) 38
Protection of Records (15.1.3) 38
Privacy and Protection of Personally Identifiable Information (15.1.4) 38
Regulation of Cryptographic Controls (15.1.5) 38
Information Security Reviews (15.2) 39
Independent Review of Information Security (15.2.1) 39
Compliance with Security Policies and Standards (15.2.2) 39
Technical Compliance Review (15.2.3) 39

16. HUMAN RESOURCE 40

Prior to Employment (16.1) 40
Screening (16.1.1) 40
Acceptable Use Policy (16.1.2) 40
During Employment (16.2) 40
Management Responsibilities (16.2.1) 40
Information Security Awareness, Education and Training (16.2.2) 40

17. VERSION HISTORY 41

18. TERMS AND DEFINITIONS 42

1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the confidentiality, integrity and availability of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been created to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by, or operated on behalf of the State of Tennessee. The methodologies and practices of external entities that require access to the State of Tennessee's information resources may be impacted and could be included in this scope. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

This document applies to all full- and part-time employees of the State of Tennessee, all third parties, contractors or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency information technology (IT) professionals and approval by the Chief Information Security Officer (CISO) and executive management team within the Office for Information Resources, Department of Finance and Administration.

All information resources and any information system owned by the State of Tennessee should be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the State government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

All of the approved policies will support the requirements of the Information Systems Council of the State of Tennessee.

2. INTRODUCTION

The Information Security Challenge

Information technology (IT) solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and technologies that support business processes at a low cost is a foundational component of successful IT programs. This integration moves quickly to align itself with the "just in time" requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes bypassing existing processes to meet time demands of the customers whom they serve. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need to evaluate risk and has established information security programs. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy to list a few.

Security policies are a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 27002 standard framework. The policies are designed to comply with applicable statutes and regulations; however, if there is a conflict, applicable statutes and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment.

Scope (2.1)

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) controlled by or operated on behalf of the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

All full- and part-time employees of the State of Tennessee, all third parties, contractors, or vendors who work on state premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data should adhere to the policies and requirements set forth in this document.

Authority (2.2)

The Information Systems Council (ISC) has authorized the Department of Finance and Administration, Office for Information Resources (OIR) to establish and enforce enterprise policies and standards as they are related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. The Office for Information Resources is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

Reference:

Tennessee Code Annotated, Section 4-3-5501, effective, May 10, 1994
ISC Information Resource Policies, Policy 1.00
ISC Information Resource Policies, Policy 13.00

Exceptions (2.3)

All exceptions to any of the security policies will be reviewed, evaluated and processed by a member of the Chief Information Security Officer's staff.

Review (2.4)

Review of this document takes place within Security Advisory Council sessions and will occur on an annual basis at a minimum. Document review can also be requested by sending a request to the Chief Information Security Officer.

The official policy document and supporting documentation will be published on the OIR intranet site located at:

http://intranet.tn.gov/finance/oir/security/policy.html

Document Format (2.5)

This document generally follows the International Standards Organization (ISO) 27002 (2013) standard framework for information technology security management. Each section starts with a high-level security control category followed by the control objective. Policy statements follow the objectives.

The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise.

X. Section Name

Control Category (x.x)
Objective Statement

Policy Name (x.x.x)
Policy Statement

Sub-Policy Name (x.x.x.x)
Sub-Policy Statement

MINIMUM COMPLIANCE REQUIREMENTS:

Policy Maintenance (2.6)

All policies will be maintained in accordance with the OIR policy process documentation.

3. INFORMATION SECURITY POLICIES

Management Direction for Information Security (3.1)

Objective: To provide management direction and support for information security in accordance with agency business requirements and relevant state and federal statute and regulations for the State of Tennessee's computing environments.

Policies for Information Security (3.1.1)

OIR Information Security Management will initiate and control an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.

Policies for Information Security (3.1.2)

Agencies may develop agency specific policy documents as required by agency or regulatory requirement provided the minimum requirements set forth in this document are met.

Policies for Information Security (3.1.3)

Agencies are responsible for communicating this policy document throughout their respective agencies.

4. OPERATIONS SECURITY

Operational Procedures and Responsibilities (4.1)

Objective: To protect critical State information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction to ensure correct and proper operations.

Documented Operating Procedures (4.1.1)

All agencies of the State of Tennessee and vendors or contractors acting on behalf of the State should identify, document and maintain standard security operating procedures and configurations for their respective operating environments and ensure the documentation is available to all users who need it.

Change Management (4.1.2)

Changes to information processing facilities and systems should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to ensure satisfactory control of all changes to equipment, software, configurations or procedures that affect the security of the State of Tennessee's operational environment. All written documentation generated by the change control policies and procedures should be retained as evidence of compliance.

Change Control Procedures (4.1.2.1)

Change control procedures should include authorization, risk assessment, logging, audit ability, and roll back procedures.

Capacity Management (4.1.3)

The use of resources should be monitored and tuned so that projections of future capacity requirements can be made.

Separation of Development, Testing and Operational Environments (4.1.4)

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and should not be used in development or test environments.

Protection from Malware (4.2)
Objective: Prevent the automated propagation of malicious code and contamination of environments attached to the enterprise network.

Malicious Software Control (4.2.1)

All computing platforms that are attached to the State's enterprise technology infrastructure or operated on behalf of the State should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs and rootkits. Compromised systems should be removed from the operational environment. All computing platforms that are attached to the State's enterprise technology infrastructure will participate in the State's enterprise antivirus program if antivirus signatures are available for the computing platforms. OIR Security Management reserves the right to seize any compromised system for forensic analysis.

Backup (4.3)
Objective: To prevent loss of data and to ensure data availability.

Data Backup (4.3.1)

Backup copies of data, software and system images should be taken and tested regularly in accordance with established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and State policy. Results of restore tests should be furnished to data owners with recommendations for any remedial steps found. Data owners should approve any remedial plans and timelines for implementing those remediation steps within a reasonable period not to exceed three months. Following remediation, the restore testing should be repeated and results documented to ensure that those steps mitigated all identified issues.

Logging and Monitoring 4.4)
Objective: To record events and generate evidence.

Event Logging (4.4.1)

All systems should be configured to support security event logging, recording user activities, exceptions, faults and information security events. System administrators should monitor and report inappropriate access to the OIR Customer Care Center. Mission critical systems should be configured to support automated logging to a facility that protects the integrity of the logs. Logging levels and

monitored elements will be configured in accordance with federal and state statute and regulatory requirements.

Availability and Performance Monitoring (4.4.2)

Mission critical systems should be configured to support State approved automated monitoring of system availability and performance.

Protection of Log Information (4.4.3)

Logging facilities and log information should be protected against tampering and unauthorized access.

Administrator and Logs (4.4.4)

System administrator activities should be logged and the logs protected and regularly reviewed.

Clock Synchronization (4.4.5)

Approved State of Tennessee managed enterprise network time servers should be the only State devices permitted to synchronize with external time services. All State provided or managed systems will synchronize time with approved State of Tennessee managed enterprise network time servers. All non-State provided or managed systems storing, processing or transmitting State data should be synchronized to State approved time synchronization services.

Control of Operational Software (4.5)

Objective: To ensure the integrity of operational systems.

Installation of Software on Operational Systems (4.5.1)

Only software that has been licensed and approved as a State standard software product or that has been approved as an exception through the State's architecture standards approval process should be installed on devices covered by the software's license agreement.

Patch Management (4.5.1.1)

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable

date can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Software Development Code (4.5.1.2)

Software development code cannot be installed on production systems (i.e. non-compiled software programming code)

Review of Application and Operating System Changes (4.5.1.3)

Applications and operating systems should be reviewed and tested to ensure that there is no adverse impact on operations or security when a change has been performed on the operating system. (e.g. patch).

Technical and Vulnerability Management (4.6)
Objective: To prevent the exploitation of technical vulnerabilities.

Management of Technical Vulnerabilities (4.6.1)

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk to the State and appropriate measures implemented to address the associated risk.

Restrictions on Software Installation (4.6.2)

Users should not install software that has not been approved by OIR and their agency.

Information Systems Audit Considerations (4.7)
Objective: To minimize the impact of audit activities on operational systems.

Information Systems Audit Controls (4.7.1)

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

5. ACCESS CONTROL

Business Requirements of Access Control (5.1)

Objective: To limit access to information and information processing facilities.

Access Control Policy (5.1.1)

All access rules and requirements to access the State of Tennessee's information resources should be developed, documented and maintained by their respective resource owners. Access to the State of Tennessee's information resources will be granted consistent with the concept of least privilege. All information processing systems owned by or operated on behalf of the State of Tennessee should have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use.

Access to Networks and Network Services (5.1.2)

All access and connectivity to the State of Tennessee's enterprise network or networks operated on behalf of the State should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

Remote Access (5.1.2.1)

All users who are accessing the State's internal network should access those resources through a State approved site-to-site Virtual Private Network (VPN) connection or through a multifactor VPN solution. All users who access State data on networks operated on behalf of the State should use secure connection methods.

Information Security Roles and Responsibilities (5.1.3)

All information security responsibilities should be defined and assigned by the access granting authority.

Segregation of Duties (5.1.4)

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse of the State's assets.

User Access Management (5.2)

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

User Registration and De-Registration (5.2.1)

A formal user registration and de-registration process should be implemented to enable assignment of access rights and to adjust those rights as the user's role changes.

User Access Provisioning (5.2.2)

User access to information resources should be authorized and provisioned according to the Agency's employee provisioning process.

User Account Naming (5.2.2.1)

All State user accounts will follow a State approved standardized naming convention.

Management of Privileged Access Rights (5.2.3)

Users should have the least privileges required to perform their roles as identified and approved by their agency. The allocation and use of privileged access rights should be restricted and controlled.

Management of Secret Authentication of Information Users (5.2.4)

The allocation of secret authentication information should be controlled through a formal management process.

Review of User Access Rights (5.2.5)

A user's access rights should be reviewed, validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies).

Removal or Adjustment of Access Rights (5.2.6)

All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day.

User Responsibilities (5.3)

Objective: To make users accountable for safeguarding their authentication information.

Use of Secret Authentication Information (5.3.1)

Users should follow State policy in the use of secret authentication information.

System and Application Access Control (5.4)

Objective: To prevent unauthorized access to systems and applications.

Information Access Restriction (5.4.1)

Access to information and application system function should be restricted in accordance with the defined access control policy.

Secure Log-on Procedures (5.4.2)

Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

System Administrator Access (5.4.2.1)

All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in State managed data processing facilities or facilities operated on behalf of the State must use a multifactor VPN solution to obtain access.

Logon Banner (5.4.2.2)

All systems and devices owned and operated by or on behalf of the State of Tennessee must display the State approved logon banner before the user is able to log in.

Service Account Use (5.4.2.3)

Service accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

Password Management System (5.4.3)

Password management systems should be interactive and should ensure quality passwords.

Use of Privileged Utility Programs (5.4.4)

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Access Control to Program Source Code (5.4.5)

Access to program source code should be restricted to authorized users.

Default Configurations (5.4.6)

All applications and processing devices that are attached to the State's enterprise technology infrastructure should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.

6. ASSET MANAGEMENT

Responsibility for Assets (6.1)

Objective: To identify organizational assets and define appropriate protection responsibilities.

Inventory of Assets (6.1.1)

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be created and maintained in order to protect the assets.

Ownership of Assets (6.1.2)

All information resource assets listed in the asset inventory should have an assigned owner or entity who will ensure the assets are protected in a manner consistent with their value, sensitivity and criticality to the business and operation of the State's government and those it serves or as specified by any superseding state or federal statute or regulation**.**

Acceptable Use of Assets (6.1.3)

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented and communicated to the employees and contractors who have access to those assets.

Return of Assets (6.1.4)

All employees and contractors must return all state assets in their possession upon termination of their employment or contract**.**

Asset Identification (6.1.5)

All state hardware assets will be named in accordance with the State approved standardized naming convention.

Data Classification (6.2)

Objective: To ensure the data used and managed by the State receives an appropriate level of protection commensurate with the value, importance and criticality of the data to the State.

Classification of Data (6.2.1)

Data assets owned and/or managed by the State of Tennessee should be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable state and/or federal statute or regulations to indicate the need, priorities and degree of protection it will receive. At a minimum, data will be classified as Public or Confidential.

Labelling of Data (6.2.2)

An appropriate set of procedures for labeling data assets owned and/or managed by the State of Tennessee should be developed and implemented in accordance with the State's data classification scheme.

Handling and Use of Data (6.2.3)

Procedures for handling data assets should be developed and implemented in accordance with the data classification scheme adopted by the State.

Public Data Classification and Control (6.2.3.1)

Data classified as public should be protected from unauthorized modification or destruction.

Confidential Data Classification and Control (6.2.3.3)

Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and cannot be used in development or test environments or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity and criticality to the business and operation of state government. Data classified as confidential must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.

Confidential Data on Personally Owned Devices (6.2.3.4)

Confidential data should not be stored on personally owned computing platforms or on personally owned mobile computing platforms unless managed by the State's mobile device management solution.

Confidential Electronic Messages Classification and Control (6.2.3.5)

E-mail sent from the State's domain out through the public Internet must be encrypted if it contains confidential information in the body or attachment. Confidential information should not be placed into the subject line of the message.

Payment Card Information Classification and Control (6.2.3.6)

Payment card information must be considered confidential when an individual's first name or first initial and last name are present in combination with account number, credit or debit card number, required security code, access code, or password that would permit access to an individual's financial account. (Payment Card Industry Data Security Standard
https://www.pcisecuritystandards.org/security_standards/)

The Payment Card Industry – Data Security Standards (PCI DSS) comprise a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector statutes and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional statutes, government regulations, or other legal requirements.

All payment card information stored and processed by the State, or transmitted over State networks must be in compliance with the PCI-DSS. Storage of the full Primary Account Number (PAN) on State systems is prohibited. Agencies that use payment card services should also comply with statewide accounting policies as documented by the Department of Finance and Administration, Division of Accounts.

Use of Confidential Data (6.2.3.7)

The use of confidential data will only be permitted in production systems. The use of confidential data is prohibited from training, test, and development systems.

To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities. Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible.

Media Handling (6.3)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on media.

Management of Removable Media (6.3.1)

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Repair of Removable Media (6.3.1.1)

Removable media should be sanitized prior to removing it from State facilities for maintenance or repair.

Disposal of Removable Media (6.3.2)

Removable media should be disposed of securely when no longer required, using approved State procedures.

Physical Transfer of Removable Media (6.3.3)

Removable media containing sensitive or confidential data must be protected against unauthorized access, misuse or corruption during transport.

Workstation Computing (6.4)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on user assigned processing devices.

State Provided Workstation Computing Platforms (6.4.1)

Workstation computing platforms, including laptops should be physically protected against theft when left unattended. Workstation computing platforms should not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a workstation computing platform should have approval from the

asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation should be encrypted while stored on the workstation computing platform.

Workstation Platform Reassignment (6.4.2)

All workstation computing platforms including all external storage devices should be sanitized prior to being re-issued or re-purposed to another employee.

Workstation Platform Disposal (6.4.3)

Hard drives in workstation computing platforms including all mobile storage devices should be sanitized using approved sanitization procedures or destroyed prior to transfer or surplus of processing device to non-State agencies.

Cloud Services (6.4.4)

Agencies and full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who are acting on behalf of the State who use cloud services for State business should seek OIR guidance and approval for proposed cloud solutions prior to enabling cloud services.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas (7.1)

Objective: To prevent unauthorized physical access, damage and interference to the State's information and information processing facilities.

Physical Security Perimeter (7.1.1)

All enterprise data processing facilities that process or store data classified as critical or sensitive should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Physical Entry Controls (7.1.2)

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

Securing Offices, Rooms and Facilities (7.1.3)

Physical security for offices, rooms and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

Protecting against External and Environmental Threats (7.1.4)

Physical protection against natural disaster, malicious attack or accidents should be considered and incorporated in facility design, construction and placement.

Working in Secure Areas (7.1.5)

Procedures for working in secure areas should be created and implemented.

Delivery and Loading Areas (7.1.6)

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

Equipment (7.2)

Objective: To prevent loss, damage, theft or compromise of assets or an interruption to State operations.

Equipment Siting and Protection (7.2.1)

Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Equipment located in areas where the State of Tennessee is unable to maintain a secure perimeter should be locked in a secured manner with access controlled by the State of Tennessee. Secured cabinets or facilities should support further segregation within the State of Tennessee's Information Technology (IT) organization based on role and responsibility.

Supporting Utilities (7.2.2)

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

Cabling Security (7.2.3)

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference or damage.

Equipment Maintenance (7.2.4)

Equipment should be correctly maintained to ensure its continued availability and integrity.

Removal of Assets (7.2.5)

All equipment, software or information that is a part of State operational systems or processes should not be taken off-site without the prior authorization from executive management or a designated representative and should be removed according to documented agency equipment transfer procedures.

Security of Equipment and Assets Off-Premises (7.2.6)

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)

All data processing equipment including storage devices subject to transfer or reuse should be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding state or federal requirements. Data processing equipment assets that are not subject to transfer or reuse should be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding state or federal requirements.

Unattended User Equipment (7.2.8)

Users should ensure that unattended data processing equipment has appropriate protection.

Session Time Outs (7.2.8.1)

All systems and devices owned and operated by or on behalf of the State of Tennessee should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

Clear Desk and Clear Screen Policy (7.2.9)

All data classified as confidential must be stored in a locked cabinet or room when unattended. All data processing equipment that provide access to Information Processing Systems will be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended.

All computing platforms residing in non-secured facilities with attached displays should be oriented away from direct line of sight from unauthorized viewers.

8. NETWORK CONNECTIVITY SECURITY

Network Security Management (8.1)

Objective: To ensure the protection of the State's assets that are accessible by suppliers and vendors.

Network Controls (8.1.1)

Networks should be managed and controlled to protect information in systems and applications.

Security of Network Services (8.1.2)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Segregation in Networks (8.1.3)

All enterprise network architectures operated by, or on behalf of, the State of Tennessee should be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones should be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the OIR Security Management Team.

Information Transfer (8.2)

Objective: To maintain the security of information transferred within network infrastructures manage by on behalf of the State and with any external entity.

Information Transfer Policies and Procedures (8.2.1)

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements on Data Transfer Policies (8.2.2)

Agreements should address the secure transfer of business information between the State and external parties.

Electronic Messaging (8.2.3)

Data involved in electronic messaging should be appropriately protected.

Internal Electronic Messages Control (8.2.3.1)

Email and instant messages internal to the State's domain containing confidential data should be encrypted during transmission. Confidential information should not be placed into the subject line of email or as any part of instant messages.

External Electronic Messages Control (8.2.3.2)

E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.

Electronic Messaging Management (8.2.3.3)

All electronic messages created, sent or received in conjunction with the transaction of official business should use the State approved gateway(s) to communicate via the Internet.

Confidentiality or Non-Disclosure Agreements (8.2.4)

When exchanging or sharing information classified as Sensitive or Confidential with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party.

Note: Agencies should work with agency legal counsel to ensure proper language is used.

9. MOBILE DEVICE SECURITY POLICY

Mobile Devices and Teleworking (9.1)

Objective: To ensure the security of teleworking and the use of mobile devices.

Mobile Device Policy (9.1.1)

All mobile devices that connect to State of Tennessee managed data or infrastructure should be managed by the State's enterprise mobile device management solution or the State's enterprise configuration manager and should comply with appropriate mobile device usage policies as required by state or federal statute or regulation.

Teleworking (9.1.2)

Teleworkers should comply with the appropriate telework policies as required by state or federal statute, regulation, state or agency policy.

10. EXTERNAL PARTY SECURITY

Information Security for External Party Relationships (10.1)

Objective: To ensure the protection of the State's assets that are accessed, processed, communicated to, or managed by external parties, suppliers or vendors. This includes any external party who has access to physical data processing facilities, logical access to State data processing systems via local or remote access or access via another external party into the State's data processing facilities.

Information Security Policy for External Party Relationships (10.1.1)

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the State's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, executive orders, standards, controls and regulations.

Identification of Risk (10.1.2)

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any State of Tennessee information, information technology asset or information process facility.

Addressing Security within External Party Agreements (10.1.3)

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for the State's processing systems or infrastructure.

Reporting of Security Incidents (10.1.3.1)

External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of State data immediately.

Sub-Contractors Requirements (10.1.3.2)

Primary external parties should require their sub-contractors to abide by State of Tennessee policies and security requirements, as applicable.

Addressing Security for Access to Citizen Data (10.1.4)

Risk involving external party access to citizen data should be identified and proper controls implemented prior to the granting of access to any State of Tennessee citizen data. Appropriate controls should be agreed upon, documented in external party agreements and implemented prior to the granting of access to any citizen data.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security Requirements of Information Systems (11.1)

Objective: To ensure that information security is an integral part of information systems throughout their life cycle. This includes application infrastructure, vendor applications, agency-developed, and user-developed applications and information systems which provide services over public networks or the State's internal network.

Security Requirements of Information Systems (11.1.1)

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance and disposal phases.

Securing Application Services on Public Networks (11.1.2)

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

Protecting Application Services Transactions (11.1.3)

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Information Security in Project Management (11.1.4)

Information security should be addressed at project initiation and throughout the lifecycle of the project.

Security in Development and Support Processes (11.2)

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

Security Requirements of Information Systems (11.2.1)

Requirements, rules and guidelines for the development of software and systems should be established and applied to all systems development.

Security in Application Systems Development (11.2.1.1)

Input validation, authentication, and authorization should be included in the design, development and implementation of applications.

Input and Data Validation (11.2.1.2)

Applications should not pass raw input to other processes including, but not limited to, other applications, web services, application server and databases. Applications should use parameterized queries or stored procedures, not dynamic SQL statements.

Output Data Validation (11.2.1.3)

Applications should not echo input back to the user or disclose information about the underlying system through error messages.

Application Authorization (11.2.1.4)

Applications that provide access to information in databases or from network shares should perform user authentication.

Inter-process Message Authentication (11.2.1.5)

Inter-process message authentication should be used to verify that a message originated from a trusted source and that the message has not been altered during transmission.

Control of Internal Processing (11.2.1.6)

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

System Change Control Procedures (11.2.2)

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Technical Review of Applications after Operating Platform Changes (11.2.3)

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Restrictions or Changes to Software Packages (11.2.4)

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

Secure System Engineering Principles (11.2.5)

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Secure Development Environment (11.2.6)

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development (11.2.7)

Outsourced system development should be monitored and supervised to ensure the State's policies and practices are followed and to ensure appropriate security controls are in place.

System Security Testing (11.2.8)

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release and prior to assigning public IP addresses or being moved or promoted into the production environment.

System Acceptance Testing (11.2.9)

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Test Data (11.3)

Objective: To ensure the protection of the data used for testing.

Protection of Test Data (11.3.1)

Test data should be selected carefully, protected and controlled. The use of production data for development and testing is prohibited.

12. BUSINESS CONTINUITY MANAGEMENT

Information Business Continuity (12.1)

Objective: To ensure the continued availability of business information and security enabled systems in the event of a crisis or disaster.

Planning Information Systems Continuity (12.1.1)

All State agencies should determine their requirements for information security and the continuity of information management systems in adverse situations, e.g. during a crisis or disaster.

Business Impact Analysis (12.1.1.1)

All State agencies should perform a Business Impact Analysis (BIA) to determine how the loss of their IT applications or information security systems would impact their business functioning and ability to deliver their core services to citizens, other agencies, and regulatory bodies.

Critical Applications (12.1.1.2)

Systems including Infrastructure components, applications and security systems identified as critical in the Business Impact Analysis will be recovered in accordance with the Business Impact Analysis and documented system recovery strategy.

Non-Critical Applications (12.1.1.3)

Infrastructure components and applications identified as non-critical in the Business Impact Analysis will be recovered on a best–effort basis. The components and applications listed as non-critical should have an explanation in the BIA justifying their low importance and demonstrating how the loss of their associated functionality will be acceptable during an event or how a manual workaround can be implemented.

Implementing Information Systems Continuity (12.1.2)

All State agencies should establish, document, implement and maintain processes, procedures and controls to ensure the required level of business continuity for all systems during an adverse situation.

Verify, Review and Evaluate information Systems Continuity (12.1.3)

All State agencies and vendors or contractors who operate on behalf of the State should verify the established and implemented information systems continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Redundancies (12.2)

Objective: To ensure availability of information processing facilities.

Availability of Information Processing Facilities (12.2.1)

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

13. INFORMATION SECURITY INCIDENT MANAGEMENT

Management of Information Security Incidents and Improvements (13.1)

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Responsibilities and Procedures (13.1.1)

The State of Tennessee will establish a Computer Security Incident Response Team (CSIRT). The CSIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The CSIRT members will be appointed based on their position and capabilities within the organization. Each agency should designate an information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC will have responsibility for incident escalations, actions and authority for the administrative oversight of security for the information technology resources under the agency's control. The POC within each agency will participate as a member of the CSIRT. The CISO of the State of Tennessee will appoint members from within OIR to participate in the CSIRT.

Reporting Information Security Events (13.1.2)

Information security events should be reported through appropriate channels using the Guidelines in the State of Tennessee Incident Response, Alerting and Communications Plan.

Data Breach and Disclosure (13.1.2.1)

Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties must provide notice of the disclosure in accordance with TCA 47-18-2107 or any other applicable state and/or federal statute or regulations).

Reporting Information Security Weakness (13.1.3)

Employees and contractors using the State's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the OIR Customer Care Center.

Assessment of and Decision on Information Security Events (13.1.4)

Information security events should be assessed and a determination made on whether to classify the event as an incident in accordance with the Incident Response Plan.

Response to Information Security Incidents (13.1.5)

Information security incidents will be managed in accordance with the documented procedures in the State of Tennessee Incident Response, Alerting and Communications Plan.

Learning from Information Security Incidents (13.1.6)

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Collection of Evidence (13.1.7)

The State should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

14. CRYPTOGRAPHY

Cryptographic Controls (14.1)

Objective: To ensure proper and effective use of cryptography to protect the confidentiality and integrity of data owned or managed by the State. Confidential information must be encrypted by the use of valid encryption processes for data at rest and in motion as required by state or federal statute or regulation. This includes but is not limited to sensitive information stored on mobile devices, removable drives and laptop computers.

Use of Cryptographic Controls (14.1.1)

Cryptographic controls should be based on the classification and criticality of the data. In deciding what strength and type of control to be deployed, both stand alone and enterprise level encryption solutions should be considered. Attention should be given to regulations, national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques.

Transmission Integrity (14.1.2)

Information systems should protect the integrity of transmitted information traveling across both internal and external communications. This control applies to communications across internal and external networks

Transmission Confidentiality (14.1.3)

Information systems should protect the confidentiality of transmitted information. The State will employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Cryptographic Module Authentication (14.1.4)

Information systems must use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal statutes, state statutes, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use will be compared to the list of NIST validated cryptographic modules quarterly to ensure compliance.

Cryptographic Module Authentication (14.1.5)

Information systems will obtain and issue public key and Secure Socket Layer (SSL) certificates from an approved service provider. This control focuses certificates with visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Key Management (14.1.6)

A secured environment should be established to protect the cryptographic keys used to encrypt and decrypt information. Cryptographic key management and establishment will be performed using automated mechanisms with supporting manual procedures. Keys should be securely distributed and stored. Access to keys should be restricted only to individuals who have a business need to access them. All access to cryptographic keys requires authorization and should be documented. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

15. COMPLIANCE

Compliance with Legal and Contractual Requirements (15.1)

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Identification of Applicable Legislation and Contractual Requirements (15.1.1)

All relevant legislative, statutory, regulatory, contractual requirements and the State's approach to meet these requirements should be explicitly identified, documented and kept current for each information system, each agency and each entity that stores, processes or transmits data on behalf of the State.

Intellectual Property Rights (15.1.2)

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products.

Protection of Records (15.1.3)

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with state or federal statutory, regulatory, contractual and business requirements.

Privacy and Protection of Personally Identifiable Information (15.1.4)

The privacy and protection of personally identifiable information should be ensured as required by relevant federal or state statute or regulation.

Regulation of Cryptographic Controls (15.1.5)

Cryptographic controls should be used in compliance with state or federal statutory, regulatory, contractual and business requirements.

Information Security Reviews (15.2)

Objective: To ensure that information security is implemented and operated in accordance the organizational policies and procedures.

Independent Review of Information Security (15.2.1)

The State's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently and at planned intervals or when significant changes occur.

Compliance with Security Policies and Standards (15.2.2)

Managers should regularly review the compliance of information processing and procedures within their area of responsibility for accuracy and applicability with the appropriate security policies, standards and any other security requirements.

Technical Compliance Review (15.2.3)

Information systems should be regularly reviewed for compliance with the State's information security policies and standards.

16. HUMAN RESOURCE

Prior to Employment (16.1)

Objective: To ensure all full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors understand their responsibilities in regards to information security requirements for the State of Tennessee's computing environments.

Screening (16.1.1)

Background and verification checks on all candidates for employment should be conducted in accordance with relevant statutes and published state policies.

Acceptable Use Policy (16.1.2)

All agencies should ensure that their full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who use State of Tennessee resources have read and accept the terms of the relevant State's Acceptable Use Policies. Proof of employee acceptance and acknowledgement will be maintained by the agency.

During Employment (16.2)

Objective: To ensure employees and contractors are aware of and fulfill their information security responsibilities.

Management Responsibilities (16.2.1)

Management should ensure that all employees and contractors are aware of and fulfill their information security responsibilities.

Information Security Awareness, Education and Training (16.2.2)

All State employees who have access to State systems and where relevant, contractors should utilize State-provided security awareness education and training when first employed and at least annually thereafter.

17. VERSION HISTORY

18. TERMS AND DEFINITIONS

Access Credentials - Access Credentials are issued to users to provide access to particular data or resources. Examples include passwords, badges, and card keys for doors.

Access Granting Authority – The access granting authority is the individual or group that has the responsibility for determining appropriate access and use of resources.

Asset – An asset is anything that can be considered a resource such as employees, computer hardware, computer software, and data.

Authentication – Authentication is the process of ensuring an individual is who they claim to be.

Authorization – Authorization is the process of providing permission to access resources or to perform operations.

Business Continuity – Business Continuity is the ability of an organization to continue its operations and services in the face of a disruptive event.

Business Impact Analysis (BIA) – A Business Impact Analysis is a process that if performed to identify and evaluate the potential impacts of natural and manmade events on business operations.

Cloud Computing – Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Confidential Data – is a generalized term that typically represents **data** classified as Confidential as defined by state or federal statute, regulation or as defined by the Payment Card Industry.

Cryptography - Cryptography is the science of transforming information into a secure form so that it can be transmitted or stored, and unauthorized persons cannot access it.

Custodian – Custodian is the individual or group that is responsible for granting access to data and or network resources.

Data Classification – Data Classification is the process of identifying the levels of protection mechanisms and restrictive access that are required for data based on state or federal statute, regulation and/or criticality and of the data.

Data Validation – Data validation is the process of ensuring that a program operates on clean, correct and useful data.

Hash – A hash is a cryptographic algorithm that can later be decrypted. It is frequently used for comparison purposes to validate the integrity of the data.

Information Systems Council (ISC) – The Information Systems Council is legislatively mandated to provide high level oversight and direction for State of Tennessee information systems and processing.

Input Validation – Input validation is a type of data validation that is applied to data from untrusted sources.

Least Privilege – Least Privilege is a practice where the minimum level of access or privileges required to perform an individual's job duties are granted.

Logic Bomb – A logic bomb is computer code that lies dormant until it is triggered by a specific logical event.

Mobile Device – A mobile device is a computing platform that not meant to be stationary. Examples include but are not limited to laptops, tablets, i-Phones, i-Pads and android devices.

Multifactor Authentication – Multifactor Authentication is using more than one factor to authenticate an individual or resource. Factors include something you know (password), something you have (token or smartcard) and something you are (biometrics such as iris or retinal scans or fingerprints).

Owner – Owner is the individual who is the final authority and decision maker in determining how data and resources are used in State business and what level of access will be granted to them.

Payment Card Industry (PCI) – The Payment Card Industry is comprised of the organizations that transmit, process or store cardholder data. The PCI works with the Payment Card Industry Security Standards Council to develop Payment Card Industry Data Security Standards.

Rootkit – A rootkit is a set of software tools used by an attacker to hide the actions or presence of other types of malicious software.

Salt - A salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase, making the stored data more difficult to crack.

Security Advisory Council – The Security Advisory Council is comprised of the directors in the Office for Information Resources.

Security Event – A security event is an event that adversely impacts the established security behavior of an environment or system

Security Incident - A security incident can be accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of State information and IT assets.

Service Account – A service account is an account that is used by systems, services or applications, not by individuals.

Trojan Horse – A trojan horse (or Trojan) is an executable program advertised as performing one activity, but actually does something else.

Virtual Private Network (**VPN**) – A VPN extends a private network across a public network, such as the Internet. It enables a computer or wireless enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Virus – A computer virus is malicious computer code that reproduces itself on the same computer.

Worm – A computer worm is a malicious program that takes advantage of a vulnerability on one computer and spreads itself to other computers with the same vulnerability.

Deliverable Specification Submission Sheet

TO:

FROM:

Project Name: **Contract Number:**

Project Manager:

The following deliverable:

is now complete. ☐ **It is available for your review**

☐ **Relevant descriptive documents are attached.**

Deliverable contract reference:

Deliverable Frequency:

Deliverable Date(s): Draft date: (if applicable) **Final:**

The deliverable is:

☐ **a document** ☐ **software** ☐ **an event** ☐ **other**

Deliverable Detail

Approval Requirements and/or reference & Deliverable description(s):
• [**Deliverable 1 - description**]

APPROVALS

Prepared By _____
Project Manager

Approved By

_____ Executive Sponsor

_____ Executive Sponsor

_____ Project Sponsor

_____ Project Sponsor

_____ State Project Manager

STATE OF TENNESSEE
Tennessee Department of Agriculture

REQUEST FOR QUALIFICATIONS # 32505-00215 AMENDMENT # 2 FOR TDA LICENSE, INSPECTION, CERTIFICATION SOFTWARE, SERVICES, AND HOSTING

DATE: 8/10/2015

RFQ # 32505-00215 IS AMENDED AS FOLLOWS:

1. **This RFQ Schedule of Events updates and confirms scheduled RFQ 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.	RFQ Issued		July 17, 2015
2.	Disability Accommodation Request Deadline	2:00 p.m.	July 22, 2015
3.	Notice of Intent to Respond Deadline	2:00 p.m.	July 24, 2015
4.	Written "Questions & Comments" Deadline	2:00 p.m.	July 31, 2015
5.	State response to written "Questions & Comments"		August 11, 2015
6.	RFQ Response Deadline	9:00 a.m.	August 25, 2015
7.	State Notice of Qualified Respondents Released		September 1, 2015
8.	State Schedules respondent Oral Presentations (Only for Qualified Respondents)		September 2, 2015
9.	Respondent Oral Presentations	8:00 a.m. – 4:30 p.m.	September 10-11, 2015
10.	RFQ Cost Negotiations		September 14-16, 2015
11.	State Evaluation Notice Released		September 17, 2015
12.	Solicitation Files Opened for Public Inspection		September 17, 2015
13.	End of Open File Period		September 24, 2015
14.	Respondent Contract Signature Deadline	2:00 p.m.	September 30, 2015

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
15.	Anticipated Contract Start Date (anticipated date for contract to be fully executed and vendor to begin work		October 15, 2015

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

STATE OF TENNESSEE
Tennessee Department of Agriculture

REQUEST FOR QUALIFICATIONS # 32505-00215 AMENDMENT # 1 FOR TDA LICENSE, INSPECTION, CERTIFICATION SOFTWARE, SERVICES, AND HOSTING

DATE: 8/7/2015

RFQ # 32505-00215 IS AMENDED AS FOLLOWS:

1. **This RFQ Schedule of Events updates and confirms scheduled RFQ 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.	RFQ Issued		July 17, 2015
2.	Disability Accommodation Request Deadline	2:00 p.m.	July 22, 2015
3.	Notice of Intent to Respond Deadline	2:00 p.m.	July 24, 2015
4.	Written "Questions & Comments" Deadline	2:00 p.m.	July 31, 2015
5.	State response to written "Questions & Comments"		August 10, 2015
6.	RFQ Response Deadline	9:00 a.m.	August 25, 2015
7.	State Notice of Qualified Respondents Released		September 1, 2015
8.	State Schedules respondent Oral Presentations (Only for Qualified Respondents)		September 2, 2015
9.	Respondent Oral Presentations	8:00 a.m. – 4:30 p.m.	September 10-11, 2015
10.	RFQ Cost Negotiations		September 14-16, 2015
11.	State Evaluation Notice Released		September 17, 2015
12.	Solicitation Files Opened for Public Inspection		September 17, 2015
13.	End of Open File Period		September 24, 2015
14.	Respondent Contract Signature Deadline	2:00 p.m.	September 30, 2015

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
15.	Anticipated Contract Start Date (anticipated date for contract to be fully executed and vendor to begin work		October 15, 2015

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

STATE OF TENNESSEE
CENTRAL PROCUREMENT OFFICE

REQUEST FOR QUALIFICATIONS
FOR
TDA LICENSE, INSPECTION, CERTIFICATION SOFTWARE, SERVICES, AND HOSTING

RFQ # 32505-00215

TABLE OF CONTENTS

SECTIONS:

1. **Introduction**
2. **RFQ Schedule of Events**
3. **Response Requirements**
4. **General Information & Requirements**
5. **Procurement Process & Contract Award**

ATTACHMENTS:

A. **Technical Response & Evaluation Guide – Mandatory Requirement Items**

B. **Technical Response & Evaluation Guide – General Qualifications & Experience Items**

C. **Technical Response & Evaluation Guide – Technical Qualifications, Experience & Approach Items**

D. **Technical Response & Evaluation Guide- Oral Presentation**

E. **Cost Proposal & Evaluation Guide**

F. **Statement of Certifications & Assurances**

G. **Reference Questionnaire**

H. ***Pro Forma* Contract**
Appendix 1 – Glossary
Appendix 2 – Functional and Technical Requirements
Appendix 3 – Statistics
Appendix 4 – Reports
Appendix 5 – Forms
Appendix 6 – Contractor Requirements
Appendix 7 – State's Acceptable Use Policy and Acceptance Use Agreement
Appendix 8 – Non-disclosure Agreement (NDA)
Appendix 9 – Public Enterprise Information Security Policies
Appendix 10 – Deliverable Specification Sheet

1. INTRODUCTION

The State of Tennessee, Central Procurement Office, hereinafter referred to as "the State," has issued this Request for Qualifications ("RFQ") to define mandatory goods or services requirements; solicit responses; detail response requirements; and outline the State's process for evaluating responses and selecting a Respondent for contract award to provide the needed goods or services.

Through this RFQ or any subsequent solicitation, the State seeks to buy the requested goods or services at the most favorable, competitive prices and to give ALL qualified businesses, including those owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises, the opportunity to do business with the State as contractors or subcontractors

1.1. Statement of Procurement Purpose

Tennessee Department of Agriculture (TDA), Division of Consumer and Industry Services (CIS) seeks to obtain an enterprise automated solution for regulatory activities in each program area, such as: licensing, inspection, certification, invoicing, revenue collection which will:

- Improve customer service to individuals and businesses in TDA,
- Provide savings through administering TDA Program Area standardization, and avoiding the cost of maintaining multiple independent systems,
- Streamline the administrative process of issuing and regulating TDA licenses, permits, inspections, and certifications.
- Provide a seamless transition from the current system(s) to the new system.
- Provide for unlimited future growth in the number of establishments in each program area.

This contract is seeking a proven Licensing, Inspection, and Certification/Education software solution, with accompanying integration, support/maintenance, and hosting services. TDA seeks an enterprise solution to automate and improve Licensing, Inspection, and Certification/Education. Please refer *to Pro Forma* Contract Appendix 2 - Functional and Technical Requirements for a narrative description of the functional requirements. The selected contractor shall provide the necessary software development tools, personnel, and project management expertise required to fulfill contractual requirements on time within the agreed project schedule. The selected Contractor will provide a solution that supports mobile devices, the mobile devices will be provided by the State.

The State is seeking a proven software solution, that is highly configurable (i.e. can be adapted to meet changing business needs with minimal custom changes to the underlying software programming code) so that TDA staff can create forms, specific workflows and business processes.

The State seeks to provide Inspectors with mobile devices to conduct both online and offline capabilities for conducting Inspections, public online access to apply for license and permit application, renewals, maintenance change needs, status, training, enforcement of rules and other critical needs via a customer web portal and employee portal with an emphasis on efficiency for enforcement services.

The State shall procure these services for the duration of the *Pro Forma* Contract and other services required to complete activities and deliverables as specified in the *Pro Forma* Contract for the project.

Background

The CIS Division is dedicated to the two main objectives of agricultural production quality and consumer protection. Responsibilities of the division include sampling the quality of feeds, seeds, and fertilizers; protecting animal and plant health; registering pesticides; ensuring food safety; and inspecting processing establishments. A laboratory supports regulatory efforts.

The TDA CIS monitors agricultural raw materials, products, and services to assure quality, consumer protection, public safety, a fair market place, and a safe and wholesome food supply. Statutes direct responsibility for the registration, licensing, sampling, inspection of items pertaining to human and animal health safety, consumer protection, truth in labeling, and free movement of plants and animals.

The vision is for a scalable enterprise solution capable of serving all TDA program areas. Currently these program areas are in several independent systems. Some of these independent systems were developed by TDA staff, and are currently maintained in-house. While other program areas, were developed and are currently supported with an outside Contractor. A few program areas and functions may still be handled manually.

The State seeks to improve its current situation through better use of technology, improved and efficient processes and workflow, improved enterprise standard policies and procedures, management and controls, and improved utilization of resources.

The State understands that implementation of an Enterprise system will necessitate organizational change management planning to support the overall implementation.

1.1.1. **Factual Data**

All statistical and fiscal information contained in this RFQ and its exhibits, including amendments and modifications thereto, are provided "as is", without warranty as to the accuracy or adequacy of the data or information so provided, and reflect the department's best understanding based on information or belief available to the department at the time of RFQ preparation. No inaccuracies in such data or information shall be a basis for delay in performance or a basis for legal recovery of damages, actual, consequential or punitive.

1.2. Notice of Intent to Respond

Before the Notice of Intent to Respond Deadline detailed in RFQ § 2, Schedule of Events, potential Respondents should submit to the Solicitation Coordinator a Notice of Intent to Respond in the form of a simple e-mail or other written communication. Such notice should include the following information: the business or individual's name (as appropriate), a contact person's name and title, the contact person's mailing address, telephone number, facsimile, number, and e-mail address. Filing a Notice of Intent to Respond is not a prerequisite for submitting a response; however, it is necessary to ensure receipt of notices and communications relating to this RFQ.

Attached to this RFQ is Appendix 8, *Non-disclosure Agreement (NDA).* Potential bidders must send in their "Intent to bid" and the signed NDA. Once the signed forms are received by the State, the State will send a copy of *Tennessee Information Resources Architecture* as referenced in RFQ Attachment H - *Pro Forma* - Section A.20. Prospective respondents must propose any exceptions to standards at the Q&A phase of the solicitation.

1.4. Definitions and Abbreviations

See RFQ Attachment H, Pro Forma Contract, Appendix 1 – Glossary.

2. RFQ SCHEDULE OF EVENTS

The following schedule represents the State's best estimates for this RFQ; however, the State reserves the right, at its sole discretion, to adjust the schedule at any time, or cancel and reissue a similar solicitation. Nothing in this RFQ is intended by the State to create any property rights or expectations of a property right in any Respondent.

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
1.	RFQ Issued		July 17, 2015
2.	Disability Accommodation Request Deadline	2:00 p.m.	July 22, 2015
3.	Notice of Intent to Respond Deadline	2:00 p.m.	July 24, 2015
4.	Written "Questions & Comments" Deadline	2:00 p.m.	July 31, 2015
5.	State response to written "Questions & Comments"		August 7, 2015
6.	RFQ Response Deadline	2:00 p.m.	August 17, 2015
7.	State Notice of Qualified Respondents Released		August 25, 2015
8.	State Schedules respondent Oral Presentations (Only for Qualified Respondents)		August 26, 2015
9.	Respondent Oral Presentations	8:00 a.m. – 4:30 p.m.	September 2-4, 2015
10.	RFQ Cost Negotiations		September 8-9, 2015
11.	State Evaluation Notice Released		September 10, 2015
12.	Solicitation Files Opened for Public Inspection		September 10, 2015
13.	End of Open File Period		September 17, 2015
14.	Respondent Contract Signature Deadline	2:00 p.m.	September 18, 2015
15.	Anticipated Contract Start Date (anticipated date for contract to be fully executed and vendor to begin work		September 30, 2015

3. RESPONSE REQUIREMENTS

3.1 Response Contents: A response to this RFQ should address the following:

3.1.1. Mandatory Requirements: This section details the mandatory technical, functional, and experience requirements that must be demonstrated in the response to this RFQ in order to be passed on to Phase II of the Technical Response evaluation. A Respondent must duplicate and use RFQ Attachment A as a guide to organize responses for the Mandatory Requirements of the RFQ response. The Respondent should reference the page location of the information within the response in the indicated column of the table. This section is included in the State's evaluation as to whether or not a Respondent meets mandatory qualifications (Phase I).

3.1.2. General Qualifications & Experience: This section is included in the State's evaluation of Phase II of the Technical Response Evaluation and details general information and qualifications that must be demonstrated in the response to this RFQ. A Respondent must duplicate and use RFQ Attachment B as a guide to organize responses for this portion of the RFQ response. The Respondent should reference the page location in the information within the response in the indicated column of the table.

3.1.3. Technical Qualifications, Experience & Approach: This section is also included in the State's evaluation of Phase II of the Technical Response Evaluation and details technical qualifications, experience, and approach items that must be demonstrated in the response to this RFQ. A Respondent must duplicate and use RFQ Attachment C as a guide to organize responses for this portion of the RFQ response. The Respondent should reference the page location in the information within the response in the indicated column of the table.

3.1.4. Cost Proposal:

3.1.4.2. If included as part of this solicitation, then the Cost Proposal must be recorded on an exact duplicate of RFQ Attachment E, Cost Proposal & Evaluation Guide. Any response that does not follow the instructions included in RFQ Attachment E may be deemed nonresponsive.

3.1.4.3. A Respondent must only record the proposed cost exactly as required by the RFQ Attachment E, Cost Proposal & Evaluation Guide and must NOT record any other rates, amounts, or information.

3.1.4.4. The proposed cost shall incorporate ALL costs for services under the contract for the total contract period.

3.1.4.5. A Respondent must sign and date the Cost Proposal.

3.1.4.6. A Respondent must submit the Cost Proposal to the State in a sealed package separate from the Technical Response.

3.2. Response Delivery Location

A Respondent must ensure that the State receives a Response to this RFQ no later than the Response Deadline time and dates detailed in the RFQ § 2, Schedule of Events. All responses must be delivered to:

Amber O'Connell
Sourcing Analyst
Central Procurement Office
Department of General Services
William R. Snodgrass TN Tower – 3rd Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615 253-7817
E-mail: Amber.OConnell@tn.gov

3.3. Response Format

3.3.1. A Respondent must ensure that the original response meets all form and content requirements detailed within this RFQ.

3.3.2. A Respondent must submit original response documents and copies as specified below.

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

"RFQ #32505-00215 TECHNICAL RESPONSE ORIGINAL"

and twenty (20) copies of the Technical Response each in the form of one (1) digital document in "PDF" format properly recorded on its own otherwise blank, standard CD-R recordable disc or USB flash drive labeled:

"RFQ #32505-00215 TECHNICAL RESPONSE COPY"

The digital copies should not include copies of sealed customer references or cost information in the general and technical evaluation phase. However, any other discrepancy between the paper response document and digital copies may result in the State rejecting the response as nonresponsive.

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

"RFQ #32505-00215 COST PROPOSAL ORIGINAL"

and one (1) copy in the form of a digital document in "XLS" format properly recorded on a separate, blank, standard CD-R recordable disc or USB flash-drive labeled:

"RFQ #32505-00215 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.

3.4. Response Prohibitions: A response to this RFQ shall not:

3.4.1. Restrict the rights of the State or otherwise qualify the response to this RFQ;

3.4.2. Include, for consideration in this procurement process or subsequent contract negotiations, incorrect information that the Respondent knew or should have known was materially incorrect;

3.4.3. Include more than one response, per Respondent, to this RFQ;

3.4.4. Include any information concerning costs (in specific dollars or numbers) associated with the Technical Response;

3.4.5. Include the respondent's own contract terms and conditions (unless specifically requested by the RFQ);

3.4.6. Include the respondent as a prime contractor while also permitting one or more other respondents to offer the respondent as a subcontractor in their own responses; or

3.4.7. Provide an oral presentation to exceed 4 hours in length including time for questions. A topic outline will be provided with the oral presentation invitation.

3.5. Response Errors & Revisions

A Respondent is responsible for any and all errors or omissions in its response to this RFQ. A Respondent will not be allowed to alter or revise its response after the Response Deadline time and dates as detailed in RFQ § 2, Schedule of Events, unless such is formally requested in writing by the State (e.g., through a request for clarification, etc.).

3.6. Response Withdrawal

A Respondent may withdraw a response at any time before the Response Deadline time and date as detailed in RFQ § 2, Schedule of Events, by submitting a written signed request by an authorized representative of the Respondent. After withdrawing a response, a Respondent may submit another Response at any time before the Response Deadline time and date as detailed in RFQ § 2, Schedule of Events.

3.7 Response Preparation Costs

The State will not pay any costs associated with the preparation, submittal, or presentation of any response. Each Respondent is solely responsible for the costs it incurs in responding to this RFQ.

4. GENERAL INFORMATION & REQUIREMENTS

4.1 Communications

4.1.1 Respondents shall reference RFQ # 32505-00215 in all communications relating to this solicitation, and direct any such communications to the following person designated as the Solicitation Coordinator:

Amber O'Connell
Sourcing Analyst
Central Procurement Office
Department of General Services
William R. Snodgrass TN Tower – 3rd Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615 253-7817
E-mail: Amber.OConnell@tn.gov

The State will convey all official responses and communications related to this RFQ to the potential respondents from whom the State has received a Notice of Intent to Respond (refer to RFQ Section 1.2.).

4.1.2 Potential respondents with a handicap or disability may receive accommodation relating to the communication of this RFQ and participating in the RFQ process. Potential respondents may contact the RFQ Coordinator to request such reasonable accommodation no later than the Disability Accommodation Request Deadline detailed in RFQ § 2, Schedule of Events.

4.1.3 **Unauthorized contact about this RFQ with other employees or officials of the State of Tennessee may result in disqualification from contract award consideration.**

4.1.4 Notwithstanding the foregoing, potential Respondents may also contact the following as appropriate:

4.1.4.1. Staff of the Governor's Office of Diversity Business Enterprise may be contacted for assistance with respect to available minority-owned, woman-owned, Tennessee service-disabled veteran-owned, and small business enterprises as well as general public information relating to this request; or

4.1.4.2. The following individual designated by the State to coordinate compliance with the nondiscrimination requirements of the State of Tennessee, Title VI of the Civil Rights Act of 1964, the Americans with Disabilities Act of 1990, and associated federal regulations:

Helen Crowley
Central Procurement Office
Department of General Services
William R. Snodgrass TN Tower – 3rd Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615 741-3836
E-mail: Helen.Crowley@tn.gov

4.2. **Nondiscrimination**

No person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of a contract pursuant to this solicitation or in the employment practices of the Vendor on the grounds of handicap or disability, age, race, color, religion (subject to *Tennessee Code Annotated,* Sections 4-21-401 and 405), sex, national origin, or any other classification protected by federal, Tennessee state constitutional, or statutory law. The Vendor pursuant to this solicitation shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

4.3. **Conflict of Interest**

4.3.1. The State may not consider a proposal from an individual who is, or within the past six (6) months has been, a State employee. For these purposes,

4.3.1.1. An individual shall be deemed a State employee until such time as all compensation for salary, termination pay, and annual leave has been paid;

4.3.1.2. A contract with or a proposal from a company, corporation, or any other contracting entity in which a controlling interest is held by any State employee shall be considered to be a contract with or proposal from the employee; and

4.3.1.3. A contract with or a proposal from a company, corporation, or any other contracting entity that employs an individual who is, or within the past six months has been, a State employee shall not be considered a contract with or a proposal from the employee and shall not constitute a prohibited conflict of interest.

4.3.2. This RFQ is also subject to *Tennessee Code Annotated*, Section 12-4-101.

4.4. **Respondent Required Review & Waiver of Objections**

4.4.1. Each potential respondent must carefully review this RFQ, including but not limited to, attachments, the RFQ Attachment H, *Pro Forma* Contract, and any amendments for questions, comments, defects, objections, or any other matter requiring clarification or correction (collectively called "questions and comments").

4.4.2. Any potential respondent having questions and comments concerning this RFQ must provide such in writing to the State no later than the written "Questions & Comments Deadline" detailed in RFQ § 2, Schedule of Events.

4.4.3. Protests based on any objection shall be considered waived and invalid if the objection has not been brought to the attention of the State, in writing, by the written "Questions & Comments Deadline."

4.5. **Disclosure of Response Contents**

4.5.1. All materials submitted to the State in response to this solicitation become property of the State of Tennessee. Selection for award does not affect this right. By submitting a response, a Respondent acknowledges and accepts that the full contents and associated documents submitted in response to this request will become open to public inspection. Refer to RFQ § 2, Schedule of Events.

4.5.2. The RFQ responses will be available for public inspection only after the completion of evaluation of the RFQ or any resulting solicitation which this RFQ becomes a part of, whichever is later.

4.6. **Notice of Professional Licensure, Insurance, and Department of Revenue Registration Requirements**

4.6.1. All persons, agencies, firms or other entities that provide legal or financial opinions, which a Respondent provides for consideration and evaluation by the State as part of a response to this RFQ, shall be properly licensed to render such opinions.

4.6.2. Before the Contract resulting from this RFQ is signed, the apparent successful Respondent (and Respondent employees and subcontractors, as applicable) must hold all necessary, appropriate business and professional licenses to provide service as required. The State may require any Respondent to submit evidence of proper licensure.

4.6.3. Before the Contract resulting from this RFQ is signed, the apparent successful Respondent must provide a valid, Certificate of Insurance indicating current insurance coverage meeting minimum requirements as may be specified by the RFQ.

4.6.4. Before the Contract resulting from this RFQ is signed, the apparent successful Respondent must be registered with the Department of Revenue for the collection of Tennessee sales and use tax. The State shall not approve a contract unless the Respondent provides proof of such registration. The foregoing is a mandatory requirement of an award of a contract pursuant to this solicitation.

4.7. **RFQ Amendments & Cancellation**

4.7.1. The State reserves the right to amend this RFQ at any time, provided that it is amended in writing. However, prior to any such amendment, the State will consider whether it would negatively impact the ability of potential respondents to meet the deadlines and revise the RFQ Schedule of Events if deemed appropriate. If a RFQ amendment is issued, the State will convey it to potential respondents who submitted a Notice of Intent to Respond (refer to RFQ § 1.2). A respondent must respond, as required, to the final RFQ (including its attachments) as may be amended.

4.7.2. The State reserves the right, at its sole discretion, to cancel or to cancel and reissue this RFQ in accordance with applicable laws and regulations.

4.8. **State Right of Rejection**

4.8.1. Subject to applicable laws and regulations, the State reserves the right to reject, at its sole discretion, any and all proposals.

4.8.2. The State may deem as nonresponsive and reject any proposal that does not comply with all terms, conditions, and performance requirements of this RFQ. Notwithstanding the foregoing, the State reserves the right to seek clarifications or to waive, at its sole discretion, a response's minor variances from full compliance with this RFQ. If the State waives variances in a response, such waiver shall not modify the RFQ requirements or excuse the Respondent from full compliance with such, and the State may hold any resulting vendor to strict compliance with this RFQ.

4.8.3. The State will review the response evaluation record and any other available information pertinent to whether or not each respondent is responsive and responsible. If the evaluation team identifies any respondent that appears <u>not</u> to meet the responsive and responsible thresholds such that the team would not recommend the respondent for potential contract award, this determination will be fully documented for the record. ("Responsive" is defined as submitting a response that conforms in all material respects to the RFQ. "Responsible" is defined as having the capacity in all respects to perform

fully the contract requirements, and the integrity and reliability which will assure good faith performance.)

4.9. **Assignment & Subcontracting**

4.9.1. The vendor may not subcontract, transfer, or assign any portion of the Contract awarded as a result of this RFQ without prior approval of the State. The State reserves the right to refuse approval, at its sole discretion, of any subcontract, transfer, or assignment.

4.9.2. If a Respondent intends to use subcontractors, the response to this RFQ must specifically identify the scope and portions of the work each subcontractor will perform (refer to RFQ Attachment B, Item B.14.).

4.9.3. Subcontractors identified within a response to this RFQ will be deemed as approved by the State unless the State expressly disapproves one or more of the proposed subcontractors prior to signing the Contract.

4.9.4. The Contractor resulting from this RFQ may only substitute another subcontractor for a proposed subcontractor at the discretion of the State and with the State's prior, written approval.

4.9.5. Notwithstanding any State approval relating to subcontracts, the Contractor resulting from this RFQ will be the prime contractor and will be responsible for all work under the Contract.

4.10. **Next Ranked Respondent**

The State reserves the right to initiate negotiations with the next ranked respondent should the State cease doing business with any respondent selected via this RFQ process.

5. PROCUREMENT PROCESS & CONTRACT AWARD

5.1. The complete vendor selection will be three-part process: (1) Qualification of Technical Responses; (2) Oral Presentation; and (3) Cost Proposals/Negotiations. Any contract award is subject to successful contract negotiation.

5.2. Qualification of Technical Responses: Technical Responses will be short-listed for further evaluation, analysis or negotiation if they are apparently responsive, responsible, and within the competitive range. A Technical Response will be deemed within the competitive range based on the following criterion:

Ranking: To be qualified for the competitive range, the Technical Response must be ranked in the top 4 after the Technical Response score is totaled and put in ordinal ranking (1 - the best evaluated ranking).

Phase I: The State will evaluate the Mandatory Requirements set forth in RFQ Attachment A on a pass/fail basis

Phase II: Following the Phase I evaluation, the State will apply a standard equitable evaluation model, which will represent a qualitative assessment of each response. Each response will be scored by Evaluation Team members according to the Technical Response & Evaluation Guides (See RFQ Attachments B & C.

The Solicitation Coordinator will total the average score from the Evaluation Team for each responsive and responsible Respondent's Technical Response Points for RFQ Attachments B & C. This will determine which of the Respondents are considered Qualified and within the competitive range.

Phase III: The State may invite those within the competitive range after Phase II evaluation to give oral presentations to the State. The qualitative assessment of each Respondent will include the information derived from the oral presentations.

5.3. Oral Presentation: The Solicitation Coordinator will invite each Respondent, who passed Phase II, to make an oral presentation.

5.3.1 The Solicitation Coordinator will schedule Respondent presentations during the period indicated by the RFQ Section 2, Schedule of Events. The Solicitation Coordinator will make every effort to accommodate each Respondent's schedules. When the Respondent presentation schedule has been determined, the Solicitation Coordinator will contact Respondents with the relevant information as indicated by RFQ Section 2, Schedule of Events.

5.3.2 Respondent presentations are only open to the invited Respondent, Proposal Evaluation Team members, the Solicitation Coordinator, and any technical consultants who are selected by the State to provide assistance to the Proposal Evaluation Team.

5.3.3 Oral presentations provide an opportunity for Respondents to explain and clarify their responses. Respondents must not materially alter their responses and presentations will be limited to addressing the items detailed in RFQ Attachment s A, B, and C, Technical Response & Evaluation Guides. Respondent pricing shall not be discussed during oral presentations. Evaluators may adjust Respondents' Technical Response scores based on Oral Presentations.

5.3.4 The State will maintain an accurate record of each Respondent's oral presentation session. The record of the Respondent's oral presentation shall be available for review

when the State opens the procurement files for public inspection.

5.4. Cost Proposals: The Cost Proposal containing the lowest cost will receive the maximum number of points per each section. See RFQ Attachment E, Cost Proposal & Evaluation Guide.

5.5. Clarifications and Negotiations: The State reserves the right to award a contract on the basis of initial responses received; therefore, each response should contain the respondent's best terms from a technical and cost standpoint. However, the State reserves the right to conduct clarifications or negotiations with respondents. All communications, clarifications, and negotiations shall be conducted in a manner that supports fairness in response improvement.

5.5.1 Clarifications: The State may identify areas of a response that may require further clarification or areas in which it is apparent that there may have been miscommunications or misunderstandings as to the State's specifications or requirements. The State may seek to clarify those issues identified during one or multiple clarification round(s). Each clarification sought by the State may be unique to an individual respondent.

5.5.2 Negotiations: The State may elect to negotiate with Qualified Respondents, within the competitive range, by requesting revised responses, negotiating costs, or finalizing contract terms and conditions. The State reserves the right to conduct multiple negotiation rounds.

5.5.2.1 Cost Negotiations: All responsive respondents within the competitive range will be given equivalent information with respect to cost negotiations. All cost negotiations will be documented for the procurement file. Additionally, the State may conduct target pricing and other goods or services level negotiations. Target pricing may be based on considerations such as current pricing, market considerations, benchmarks, budget availability, or other methods that do not reveal individual respondent pricing. During target price negotiations, respondents are not obligated to meet or beat target prices, but will not be allowed to increase prices.

5.5.2.2 If the State determines costs and contract finalization discussions and negotiations are not productive, the State reserves the right to bypass the apparent best evaluated Respondent and enter into contract negotiations with the next apparent best evaluated Respondent.

5.6. Evaluation Guide

The State will consider qualifications, experience, technical approach, and cost (if applicable) in the evaluation of responses and award points in each of the categories detailed below. The maximum evaluation points possible for each category are detailed below.

Evaluation Category	Maximum Points Possible
Mandatory Requirements (refer to RFQ Attachment A)	Pass/Fail
General Qualifications, Experience (refer to RFQ Attachment B)	20
Technical Qualifications & Approach (refer to RFQ Attachment C)	40
Oral Presentation (refer to RFQ Attachment D)	10
Cost Proposal (refer to RFQ Attachment E)	30

5.7. Contract Award

5.7.1. The Solicitation Coordinator will submit the Evaluation Team determinations and response scores to the head of the contracting agency, or the agency head's designee, for consideration along with any other relevant information that might be available and pertinent to contract award.

5.7.2. The contracting agency head, or the agency head's designee, will determine the apparent best-evaluated response. (To effect a contract award to a Respondent other than the one receiving the highest evaluation score, the head of the contracting agency must provide written justification and obtain written approval of the Chief Procurement Officer and the Comptroller of the Treasury.)

5.7.3. The State reserves the right to make an award without further discussion of any response.

5.7.4. The State will issue an Evaluation Notice and make the RFQ files available for public inspection at the time and date specified in the RFQ §2, Schedule of Events.

NOTICE: The Evaluation Notice shall not create rights, interests, or claims of entitlement in either the Respondent identified as the apparent best evaluated or any other Respondent.

5.7.5. The Respondent identified as offering the apparent best-evaluated must sign a contract drawn by the State pursuant to this RFQ. The contract shall be substantially the same as the RFQ Attachment H, *Pro Forma* contract. The Respondent must sign said contract no later than the Respondent Contract Signature Deadline detailed in RFQ § 2, Schedule of Events. If the Respondent fails to provide the signed contract by the deadline, the State may determine the Respondent is non-responsive to this RFQ and reject the response.

5.7.6. Notwithstanding the foregoing, the State may, at its sole discretion, entertain limited negotiation prior to contract signing and, as a result, revise the *Pro Forma* contract terms and conditions or performance requirements in the State's best interests, PROVIDED THAT such revision of terms and conditions or performance requirements shall NOT materially affect the basis of response evaluation or negatively impact the competitive nature of the RFQ and vendor selection process.

5.7.7. If the State determines that a response is nonresponsive and rejects it after opening Cost Proposals, the Solicitation Coordinator will re-calculate scores for each remaining responsive Cost Proposal to determine (or re-determine) the apparent best-evaluated response.

TECHNICAL RESPONSE & EVALUATION GUIDE

All Respondents must address all items detailed below and provide, in sequence, the information and documentation as required (referenced with the associated item references). All Respondents must also detail the response page number for each item in the appropriate space below.

The Solicitation Coordinator will review all responses to determine if the Mandatory Requirement Items are addressed as required and mark each with pass or fail. For each item that is not addressed as required, the Evaluation Team must review the responses and attach a written determination. In addition to the Mandatory Requirement Items, the Solicitation Coordinator will review each response for compliance with all RFQ requirements.

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	**Item Ref.**	**Section A— Mandatory Requirement Items**	**Pass/Fail**
		The Technical Response must be delivered to the State no later than the Technical Response Deadline specified in the RFQ § 2, Schedule of Events.	
		The Technical Response must not contain cost or pricing information of any type.	
		The Technical Response must not contain any restrictions of the rights of the State or other qualification of the response.	
		A Respondent must not submit alternate responses.	
		A Respondent must not submit multiple responses in different forms (as a prime and a subcontractor).	
	A.1.	Provide the Statement of Certifications and Assurances (RFQ Attachment F) completed and signed by an individual empowered to bind the Respondent to the provisions of this RFQ and any resulting contract. The document must be signed without exception or qualification.	
	A.2.	Provide a statement, based upon reasonable inquiry, of whether the Respondent or any individual who shall perform work under the contract has a possible conflict of interest (e.g., employment by the State of Tennessee) and, if so, the nature of that conflict. NOTE: Any questions of conflict of interest shall be solely within the discretion of the State, and the State reserves the right to cancel any award.	
	A.3.	Provide a current bank reference indicating that the Respondent's business relationship with the 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.	

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	**Item Ref.**	**Section A— Mandatory Requirement Items**	**Pass/Fail**
	A.4.	Provide two current positive credit references from vendors with which the Respondent has done business written in the form of standard business letters, signed, and dated within the past three (3) months.	
	A.5.	Provide an official document or letter from an accredited credit bureau, verified and dated within the last three (3) months and indicating a positive credit rating for the Respondent (NOTE: A credit bureau report number without the full report is insufficient and will not be considered responsive).	
	A.6.	Provide a valid, Certificate of Insurance that is verified and dated within the last six (6) months and which details all of the following: (a) Insurance Company (b) Respondent's Name and Address as the Insured (c) Policy Number (d) The following minimum insurance coverage: (i) Workers' Compensation/ Employers' Liability (including all states coverage) with a limit not less than the relevant statutory amount or one million Dollars ($1,000,000) per occurrence for employers' liability; (ii) Comprehensive Commercial General Liability (including personal injury & property damage, premises/operations, independent contractor, contractual liability and completed operations/products) with a bodily injury/property damage combined single limit not less than one million Dollars ($1,000,000) per occurrence two million Dollars ($2,000,000) aggregate; (e) The following information applicable to each type of insurance coverage: (i) Coverage Description, (ii) Exceptions and Exclusions, (iii) Policy Effective Date, (iv) Policy Expiration Date, and (v) Limit(s) of Liability.	
	A.7.	Provide written confirmation that the Respondent's proposed solution will provide the features and functions or their equivalent included in Appendix 2 – Functions and Technical Requirements, to Attachment H. *Pro Forma Contract*. (This can be accomplished	

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	**Item Ref.**	**Section A— Mandatory Requirement Items**	**Pass/Fail**
		by including a copy of the completed Appendix 2)	
	A.8.	Provide written confirmation that the Project functions or functional equivalent detailed in the RFQ for Stage 1(a) will meet the TDA timeline. (See RFQ Attachment H *Pro Forma Contract* - item A.4)	
	A.9.	Provide written confirmation that the proposed solution will maintain all data at all times within the U.S.	
	A.10.	Provide written confirmation that the proposed solution will encrypt data as outlined. RFQ Attachment H - *Pro Forma Contract* - Item A.43. Encryption	
	A.11.	Provide written confirmation of the security certification as outlined in RFQ Attachment H - *Pro Forma Contract* - Item A.53. Security Certification, Accreditation Audit	
State Use – RFQ Coordinator Signature, Printed Name & Date:			

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION B: GENERAL QUALIFICATIONS & EXPERIENCE. The Respondent must address all items detailed 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. Evaluation Team members will independently evaluate and assign one score for all responses to Section B— General Qualifications & Experience Items.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
	B.1.	Detail the name, e-mail address, mailing address, telephone number, and facsimile number of the person the State should contact regarding the response.
	B.2.	Describe the Respondent's form of business (*i.e.*, individual, sole proprietor, corporation, non-profit corporation, partnership, limited liability company) and business location (physical location or domicile).
	B.3.	Detail the number of years the Respondent has been in business.
	B.4.	Briefly describe how long the Respondent has been performing the goods or services required by this RFQ.
	B.5.	Describe the Respondent's number of employees, client base, and location of offices.
	B.6.	Provide a statement of whether there have been any mergers, acquisitions, or sales of the Respondent within the last ten (10) years. If so, include an explanation providing relevant details.
	B.7.	Provide a statement of whether the Respondent or, to the Respondent's knowledge, any of the Respondent's employees, agents, independent contractors, or subcontractors, proposed to provide work on a contract pursuant to this RFQ, have been convicted of, pled guilty to, or pled *nolo contendere* to any felony. If so, include an explanation providing relevant details.
	B.8.	Provide a statement of whether, in the last ten (10) years, the Respondent has filed (or had filed against it) any bankruptcy or insolvency proceeding, whether voluntary or involuntary, or undergone the appointment of a receiver, trustee, or assignee for the benefit of creditors. If so, include an explanation providing relevant details.
	B.9.	Provide a statement of whether there is any material, pending litigation against the Respondent that the Respondent should reasonably believe could adversely affect its ability to meet contract requirements pursuant to this RFQ or is likely to have a material adverse effect on the Respondent's financial condition. If such exists, list each separately, explain the relevant details, and attach the opinion of

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		counsel addressing whether and to what extent it would impair the Respondent's performance in a contract pursuant to this RFQ. NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders such opinions.
	B.10.	Provide a statement of whether there is any pending or in progress Securities Exchange Commission investigations involving the Respondent. If such exists, list each separately, explain the relevant details, and attach the opinion of counsel addressing whether and to what extent it will impair the Respondent's performance in a contract pursuant to this RFQ. NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders such opinions.
	B.11.	Provide a brief, descriptive statement detailing evidence of the Respondent's ability to deliver the goods or services sought under this RFQ (*e.g.*, prior experience, training, certifications, resources, program and quality management systems, *etc*.).
	B.12.	Provide a narrative description of the proposed contract team, its members, and organizational structure along with an organizational chart identifying the key people who will be assigned to provide the goods or services required by this RFQ, illustrating the lines of authority, and designating the individual responsible for the completion of each task and deliverable of the RFQ.
	B.13.	Provide a personnel roster listing the names of key people who the Respondent will assign to perform tasks required by this RFQ along with the estimated number of hours that each individual will devote to the required tasks. Follow the personnel roster with a resume for each of the people listed. The resumes must detail the individual's title, education, current position with the Respondent, and employment history.
	B.14.	Provide a statement of whether the Respondent intends to use subcontractors to accomplish the work required by this RFQ, and if so, detail: (a) the names of the subcontractors along with the contact person, mailing address, telephone number, and e-mail address for each; (b) a description of the scope and portions of the work each subcontractor will perform; <u>and</u> (c) a statement specifying that each proposed subcontractor has expressly

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		assented to being proposed as a subcontractor in the Respondent's response to this RFQ.
	B.15.	Provide documentation of the Respondent's commitment to diversity as represented by the following: (a) Business Strategy. Provide a description of the Respondent's existing programs and procedures designed to encourage and foster commerce with business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises. Please also include a list of the Respondent's certifications as a diversity business, if applicable. (b) Business Relationships. Provide a listing of the Respondent's current contracts with business enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises. Please include the following information: (i) contract description; (ii) contractor name and ownership characteristics (*i.e.*, ethnicity, gender, Tennessee service-disabled); and (iii) contractor contact name and telephone number. (c) Estimated Participation. Provide an estimated level of participation by business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises if a contract is awarded to the Respondent pursuant to this RFQ. Please include the following information: (i) a percentage (%) indicating the participation estimate. (Express the estimated participation number as a percentage of the total estimated contract value that will be dedicated to business with subcontractors and supply contractors having such ownership characteristics only and **DO NOT INCLUDE DOLLAR AMOUNTS**); (ii) anticipated goods or services contract descriptions; (iii) names and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veterans) of anticipated subcontractors and supply contractors. NOTE: In order to claim status as a Diversity Business Enterprise under this contract, businesses must be certified by the Governor's Office of Diversity Business Enterprise (Go-DBE). Please visit the Go-DBE website at https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&XID=9265 for more information. (d) Workforce. Provide the percentage of the Respondent's total current employees by ethnicity and gender.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		NOTE: Respondents that demonstrate a commitment to diversity will advance State efforts to expand opportunity to do business with the State as contractors and subcontractors. Response evaluations will recognize the positive qualifications and experience of a Respondent that does business with enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises and who offer a diverse workforce.
	B.16.	Provide a statement of whether or not the Respondent has any current contracts with the State of Tennessee or has completed any contracts with the State of Tennessee within the previous five-year period. If so, provide the following information for all current and completed contracts: (a) the name, title, telephone number and e-mail address of the State contact responsible for the contract at issue; (b) the name of the procuring State agency; (c) a brief description of the contract's specification for goods or scope of services; (d) the contract term; and (e) the contract number. NOTES: ▪ Current or prior contracts with the State are not a prerequisite and are not required for the maximum evaluation score, and the existence of such contracts with the State will not automatically result in the addition or deduction of evaluation points. ▪ Each evaluator will generally consider the results of inquiries by the State regarding all contracts responsive to Section B.16 of this RFQ.
	B.17.	Provide customer references from individuals who are not current or former State employees for projects similar to the goods or services sought under this RFQ and which represent: ▪ two (2) accounts Respondent currently services that are similar in size to the State; and ▪ three (3) completed projects. Reference from at least three (3) different individuals are required to satisfy the requirements above, e.g., an individual may provide a reference about a completed project and another reference about a currently services account. The standard reference questionnaire, which must be used and completed is provided at RFQ Attachment G. References that are not completed as required may be deemed nonresponsive and may not be considered. The Respondent will be solely responsible for obtaining fully completed reference questionnaires and including them in the Respondent's sealed Technical Response. In order to obtain and submit the completed reference questionnaires

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		follow the process below: (a) Add the Respondent's name to the standard reference questionnaire at Attachment G and make a copy for each reference. (b) Send a reference questionnaire and a new standard #10 envelope to each reference. (c) Instruct the reference to: (i) complete the reference questionnaire; (ii) sign <u>and</u> date the completed reference questionnaire; (iii) seal the completed, signed, and dated reference questionnaire within the envelope provided; (iv) sign his or her name in ink across the sealed portion of the envelope; and (v) return the sealed envelope directly to the Respondent (the Respondent may wish to give each reference a deadline, such that the Respondent will be able to collect all required references in time to include them within the sealed Technical Response). (d) <u>Do NOT open the sealed references upon receipt</u>. (e) Enclose all <u>sealed</u> reference envelopes within a larger, labeled envelope for inclusion in the Technical Response as required. NOTES: ▪ The State will not accept late references or references submitted by any means other than that which is described above, and each reference questionnaire submitted must be completed as required. ▪ The State will not review more than the number of required references indicated above. ▪ While the State will base its reference check on the contents of the sealed reference envelopes included in the Technical Response package, the State reserves the right to confirm and clarify information detailed in the completed reference questionnaires, and may consider clarification responses in the evaluation of references. ▪ The State is under <u>no</u> obligation to clarify any reference information.
	B.18.	Provide a statement and any relevant details addressing whether the Respondent is any of the following: (a) is presently debarred, suspended, proposed for debarment, or voluntarily excluded from covered transactions by any federal or state department or agency; (b) has within the past three (3) years, been convicted of, or had a civil judgment rendered against the contracting party from commission of fraud, or a criminal offence in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	**Item Ref.**	**Section B— General Qualifications & Experience Items**
		under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; (c) is presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed above; and has within a three (3) year period preceding the contract had one or more public transactions (federal, state, or local) terminated for cause or default.
	B.19.	Provide a list of any non-State standard products the Contractor may require which deviates from the State's Technology Architecture Product Standards document.
	B.20.	The State is amenable to making changes to RFQ Attachment H, *Pro Forma* contract. The State will take all reasonable suggested alternative or supplemental contract language changes by Respondents under advisement during the evaluation and post award processes, subject to any mandates or restrictions imposed on the State by applicable state or federal law. The State, however, recommends that Respondents include with their response any alternative or supplemental suggested contract language that a Respondent would propose. Clearly indicate, by providing a "red-line" of RFQ Attachment H, *Pro Forma* contract, all suggested alternative or supplemental contract language. Do not include any exceptions or changes that (1) contradict a Federal requirement or a Mandatory Requirement, or (2) push back any deadlines.
SCORE *(for all Section B—Qualifications & Experience Items above)* : *(maximum possible score = 20)*		
State Use – Evaluator Identification:		

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION C: TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH. The Respondent should explain its approach to providing goods or services to the State. The items listed below represent specific questions the State would request you answer in your response. For ease of review, please annotate your explanation so that it contains references to the items listed below where they are addressed. Respondent should not feel constrained to answer only the specific questions listed below in its explanation and should feel free to provide attachments if necessary in an effort to provide a more thorough response.

The Evaluation Team, made up of three (3) 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 scores 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**
Technical					
	C.1.	Provide a narrative that illustrates the Respondent's understanding of the State's requirements and project schedule.		**25**	
	C.2.	Provide a narrative that illustrates how the Respondent will complete the delivery of goods or scope of services, accomplish required objectives, and meet the State's project schedule.		**15**	
	C.3.	Provide a narrative that illustrates how the Respondent will manage the project, ensure delivery of specified goods or completion of the scope of services, and accomplish required objectives within the State's project schedule.		**25**	
	C.4.	Describe your company's approach to meet project deliverables and **required milestones** to satisfy mandatory implementation timeframe based on the defined scope and requirements RFQ		**25**	

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	**Item Ref.**	**Section C— Technical Qualifications, Experience & Approach Items**	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
		Attachment H - *Pro Forma* – Item A.4. **NOTE:** Do not include any pricing or cost structures.			
	C.5.	Provide a narrative that illustrates how the Respondent will complete the delivery of **Applications, Permits, and Renewals requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**50**	
	C.6.	Provide a narrative that illustrates how the Respondent will complete the delivery **of Billing and Fee collection requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**50**	
	C.7.	Provide a narrative that illustrates how the Respondent will complete the delivery of **Inspection Management requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**50**	
	C.8.	Provide a narrative that illustrates how the Respondent will complete the **Violation Tracking requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**25**	
	C.9.	Provide a narrative that illustrates how the Respondent will complete the **Complaint Tracking requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**25**	
	C.10.	Provide a narrative that illustrates how the Respondent will complete the **Mobile Access requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**35**	

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.11.	Provide a narrative that illustrates how the Respondent will complete the **System Common requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**35**	
	C.12.	Provide a narrative that illustrates how the Respondent will complete **Performance Data Analysis requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**35**	
	C.13.	Provide a narrative that illustrates how the Respondent will complete the **Certification Testing and Administration requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements.*		**20**	
	C.14.	Provide a narrative that illustrates how the Respondent will complete the **System Use Training requirements** as summarized in RFQ Attachment H - *Pro Forma* - Appendix 2 - *Functional & Technical Requirements* and RFQ Attachment G - *Pro Forma* - Item A.17.		**5**	
	C.15.	Provide a narrative that illustrates the Respondent understands the **State's Project Management Methodology requirements** RFQ Attachment H - *Pro Forma* – Item A.3.		**10**	
	C.16.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Organizational Change Management (OCM) requirements** as described in RFQ Attachment H - *Pro Forma* – Item A.16 and RFQ Attachment G - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 4.		**10**	

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.17.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Project Initiation Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 1. Also provide draft/example of Turnover/Transition Plan as described in Attachment H - *Pro Forma* – Item A.69.		**10**	
	C.18.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Project Management Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 2.		**10**	
	C.19.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Business Process Re-engineering Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 3.		**10**	
	C.20.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Design Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 5.		**20**	
	C.21.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Development Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 6.		**20**	
	C.22.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Acceptance Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 7.		**10**	

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.23.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **System Implementation Phase Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 8.		**10**	
	C.24.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **TDA Staff Training Requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 9.		**5**	
	C.25.	Provide a narrative describing the Respondent's understanding of and ability to satisfy **TDA Staff Training Estimates** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 10.		**5**	
	C.26.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **Maintenance and Support requirements** as described in RFQ Attachment H - *Pro Forma* – Appendix 6 – Contractor Requirements, Table 11.		**15**	
	C.27.	Provide a narrative describing the Respondent's understanding of and ability to satisfy the **System Warranty of System Products/Services requirements** as described in RFQ Attachment H - *Pro Forma* - Item A.18.		**10**	
	C.28.	Provide a narrative that describes the customary division of support between the vendor and the customer. Include standard roles and responsibilities definitions for both the vendor and the customer for new application releases, upgrades, and administrative functions.		**5**	

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.29.	Provide a narrative that describes the customary product maintenance and enhancement cycle.		**10**	
	C.30.	Provide a narrative that describes the process involved in implementing your product for a new customer of similar size and scope of implementation as the State is envisioning.		**25**	
	C.31.	Provide a narrative that describes the additional support services provided. Do not include ANY pricing in response to this question.		**10**	
	C.32.	Provide a narrative that describes the **staffing requirements to be met by the State** in order to meet the schedule as described in RFQ Attachment H - *Pro Forma* - Item A.7. Provide a description of the skills required and the quantities and levels of commitment for each skill.		**5**	
	C.33.	Provide a narrative that illustrates how the Respondent how the Respondent has completed the delivery of a Mobile solution, in a similar size project Describe your experience in implementation including the following: • *How long has the Mobile solution been in production?* • *How many implementations in the past 5 years included a mobile solution?* • *Provide the type and number of mobile clients.* ***Client information:*** • *Type of client (e.g. government entity (local, State, Federal), private company etc.);* • *Number of back-office users;*		**20**	

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	**Item Ref.**	**Section C— Technical Qualifications, Experience & Approach Items**	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
		• *Number of licensees with online accounts;* • *Total number of licensees;* • *Number of license types;* • *Number of locations;* • *Number of licensing entities;* • *Annual licensing revenues; and* • *Any other information relevant to describing the client organization(s) in the context of this Competitive Negotiation* ***Project information:*** • *Project including original estimates and final budget* • *Project duration including start/end dates; including original estimates and final project duration.* • *Number of Contractor staff (Full Time Employees) involved in the implementation; and* • *Number of client staff (FTEs) involved in the implementation.*			
	C.34.	Provide a narrative that Illustrates how the proposed system will provide a **Third Party Cashiering System not excluding the State Authorized Card Credit Card processor, and the State's cashiering system (iNovah)** as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common – System Interface. Appendix 2 – Bill & Fee Collection – Fees and Fines Collection Appendix 2 – Bill & Fee Collection – On-line Payment.		**5**	
	C.35.	Provide a narrative that illustrates how the proposed system will provide **Document Management**, to include scanning, uploading, attaching, document metadata, document lookup/retrieval, document retention, document archiving, version control, etc. as defined in RFQ Attachment H - *Pro Forma* - Item A.56.		**20**	

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.36.	Provide a narrative that Illustrates how the proposed system will provide **interface methods and tools with other non TDA systems** (i.e. State's USALIMS system, Third party Lab results, Revenue, etc.) as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	
	C.37.	Provide a narrative that Illustrates how the proposed system will **provide electronic signature** as defined in RFQ Attachment H - *Pro Forma* – Appendix 2 – Applications, Permits & Renewal – License Application. Appendix 2– Mobile Access.		**5**	
	C.38.	Provide a narrative that Illustrates how the proposed system will provide **compliance with Payment Card Industry (PCI) and 508 Compliance requirements** as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common - Security.		**5**	
	C.39.	Provide a narrative that Illustrates how the proposed system will **provide automated business rules** as required in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	
	C.40.	Provide a narrative that Illustrates how the proposed system will **provide system notifications** - via text message or emails as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	
	C.41.	Provide a narrative that Illustrates how the proposed system will provide **audit trail functionality** to track the details of all events that occur within the system including any addition, change, or deletion of data as defined in RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common.		**5**	

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.42.	Provide a narrative detailing how the contractor will develop detailed **system documentation** described in RFQ Attachment H - *Pro Forma* - Item A.21. System documentation differs from training materials in that it defines the system architecture, explains project implementation activities, and demonstrates how the system can be tailored over time to fit evolving needs of the State.		**5**	
	C.43.	Provide a narrative detailing how well your **Help Desk** processes match the business needs outlined in RFQ Attachment H - *Pro Forma* – Item A.22.. Specifically address each sub section: hours of operation, communication methods, level of staff knowledge, and incident resolution procedures.		**10**	
	C.44.	Describe (without revealing cost) the **User Licensing**, including any Third Party software, necessary to support the System, the types of licenses and numbers of license necessary to support all users, disaster recovery, and non-production environments, including training in RFQ Attachment H - *Pro Forma* - Item A.23.		**10**	
	C.45.	Provide a narrative detailing your network architectural design "without revealing proprietary details or trade secrets."		**5**	

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.46.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections: A.34. Legal Compliance A.36. Miscellaneous Security Provisions (including who is doing the scans) A.41. Data Ownership A.42. Data Location A.44. Import and Export of Data A.68. Termination or Suspension of Service A.69. Turnover Plan A.75. Data and System Conversion		**30**	
	C.47.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections: A.39. Protection of Information		**10**	
	C.48.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections: A.43. Encryption		**10**	
	C.49.	Provide a narrative detailing how your solution will comply with the Data requirements as listed in RFQ Attachment H - *Pro Forma* Sections A.45. Data Protection A.46. Industry Data Security Standard		**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)*	

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	**Item Ref.**	**Section C— Technical Qualifications, Experience & Approach Items**	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
Total Raw Weighted Score / **Maximum Possible Raw Weighted Score** *(i.e., 5 x the sum of item weights above)*			**X 40** *(maximum possible score)*	**= SCORE:**	
State Use – Evaluator Identification:					
State Use – Solicitation Coordinator Signature, Printed Name & Date:					

TECHNICAL RESPONSE & EVALUATION GUIDE

Attachment D: ORAL PRESENTATION. The Respondent must address ALL Oral Presentation Items (below).

A Proposal Evaluation Team, made up of three or more State employees, will independently evaluate and score the presentation 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:			
Oral Presentation Items	**Item Score**	**Evaluation Factor**	**Raw Weighted Score**
D.1. Demo Application, License/Permits & Renewals		**5**	
D.2. Demo Inspections (mobile devices online/offline, assigning inspections to inspectors, etc)		**5**	
D.3 Demo Bill and Fee Collections		**5**	
D.4 Demo Third Party Laboratory lab results transferred into system		**2**	
D.5 Demo setting up a new user		**2**	
D.6 Demo Document Management Capabilities		**5**	
D.7 Demo Certification Testing and Administration		**4**	
D.8 Demo rule based alerts		**3**	
D.9 Demo maintaining business rules in the system		**5**	
D.10 Describe the security certifications of Vendor and their Subcontractors		**2**	
D.11 Describe lessons learned regarding migrating current date into the new system		**3**	
D.12 Describe the Organizational Change that has occurred with business processes, job roles, and organizational structure with the implementation of the system		**5**	
Total Raw Weighted Score *(sum of Raw Weighted Scores above)***:** The Solicitation Coordinator will use this sum and the formula below to calculate the score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.			

RESPONDENT LEGAL ENTITY NAME:	

total raw weighted score / **maximum possible raw weighted score** *(i.e., 5 x the sum of item weights above)*	**X 10** *(maximum section score)*	**= SCORE:**	

State Use – Evaluator Identification:
State Use – Solicitation Coordinator Signature, Printed Name & Date:

Cost Proposal & Evaluation 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 the delivery of specified goods for the entire scope of services including all services defined in the Scope of Services of the RFQ Attachment H, *Pro Forma* Contract and for the entire contract period. The Cost Proposal shall remain valid for at least 120 days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract resulting from this RFQ. All monetary amounts shall be in U.S. currency and limited to two (2) places to the right of the decimal point.

NOTICE: The Evaluation Factor associated with each line item of cost 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 line item of costs herein, pursuant to the second paragraph of the *pro forma* contract section C.1. (refer to RFQ Attachment H), "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 entity responding to the provisions of this RFQ and any contract awarded pursuant thereto. If said individual is not responding in an individual capacity or is the *President* or *Chief Executive Officer*, this document must attach evidence showing the individual's authority to legally bind the entity responding to this RFQ.

RESPONDENT SIGNATURE:	
PRINTED NAME & TITLE:	
DATE:	

RESPONDENT LEGAL ENTITY NAME:		
Cost Item Description **(Cost for all Stages – see RFQ attachment H – item-A.4)**	**Proposed Cost** **DDI through Retainage Period**	**State Use ONLY**
1. Design, Development, and Implementation (DDI)	$	
2. Post-Implementation Support and Maintenance (Stage 1 through Retainage)	$	
3. Post-Implementation Hosting (Stage 1 through Retainage)	$	
The RFQ Coordinator will use this sum and the formula below to calculate the Part A Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations	**Total System Cost** **(Part A Evaluation Cost Amount):** *(Sum of Proposed Costs Above)*	
Lowest Part A Evaluation Cost Amount from <u>all</u> Proposals **Part A Evaluation Cost Amount Being Evaluated**	**x 20** *(maximum section score)* **= PART A SCORE:**	
State Use ONLY – RFQ Coordinator Signature, Printed Name & Date:		

RESPONDENT LEGAL ENTITY NAME:									
Recurring Annual Costs for Hosting, Support and Maintenance. **(Please list the cost post retainage period. The State will sum rows and record the sum in the "State Use Only" column.)**	**Proposed Cost - Hosting, Support and Maintenance (Post Retainage)**								**State Use ONLY**
	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Optional Year 1**	**Optional Year 2**	**Optional Year 3**	**Evaluation Cost**
Hosting (includes 250 User Licensing for TDA users)	$	$	$	$	$	$	$	$	
Support and Maintenance	$	$	$	$	$	$	$	$	
User Licensing Fee for each additional 10 TDA users post retainage period.	$	$	$	$	$	$	$	$	
The RFQ Coordinator will use this sum and the formula below to calculate the Part B Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.								**Part B Evaluation Cost Amount:** *(Sum of Evaluation Costs Above)*	
Lowest Part B Evaluation Cost Amount from all Proposals / **Part B Evaluation Cost Amount being evaluated**				**x 8** *(maximum section score)*				**= PART B SCORE:**	
State Use ONLY – RFQ Coordinator Signature, Printed Name & Date:									

RESPONDENT LEGAL ENTITY NAME:	

CHANGE ORDER RATES SCHEDULE

The hourly change order rates, detailed below, shall indicate the proposed rates for processing all State-approved additional work. All monetary amounts are United States currency.

NOTE: The costs proposed must be fully loaded to cover travel, meals, and lodging expenses associated with providing the services; the State will not pay travel-related expenses separately.

The Proposer may enter zero (0) in a required Proposed Hourly Rate cell; however, the Proposer must not leave any required Proposed Rate cell blank. For evaluation and contractual purposes, the State shall interpret a blank Proposed Rate cell as zero (0).

NOTE: In Contract Section C.3.c, there is a seven percent (7 %) cap on the total amount of Additional Work that can be procured without amending the contract for additional funds. However, this cap is for contractual purposes only and does not apply to, or in any way restrict, the change order amounts that the vendor may propose below.

Cost Item Description	**Proposed Cost**	**State Use ONLY**	
		Evaluation Factor ***(Note: Actual usage is unknown. The evaluation factors below are estimated usage for cost evaluation only.)**	**Evaluation Cost** **(cost x factor)**
Project Manager	$ /HOUR	150	
Business Analyst	$ /HOUR	200	
Technical Manager/Lead	$ /HOUR	400	
Developer	$ /HOUR	800	
The RFQ Coordinator will use this sum and the formula below to calculate the Part C Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.		**Part C Evaluation Cost Amount:** *(Sum of Evaluation Costs Above)*	

Lowest Part C Evaluation Cost Amount from all Proposals / **Part C Evaluation Cost Amount being evaluated**	**x 2** *(maximum section score)*	**= PART C SCORE:**	
FINAL SCORE (TOTAL OF PART A, PART B, AND PART C):			

State Use ONLY – RFQ Coordinator Signature, Printed Name & Date:

STATEMENT OF CERTIFICATIONS AND ASSURANCES

An individual responding in his or her individual capacity or legally empowered to contractually bind the Respondent must complete and sign the Statement of Certifications and Assurances below as required, and this signed statement must be included with the response as required by the Request for Qualifications.

The Respondent does, hereby, expressly affirm, declare, confirm, certify, and assure ALL of the following:

1. The Respondent will comply with all of the provisions and requirements of the RFQ.
2. The Respondent will provide all specified goods or services as required by the contract awarded pursuant to this RFQ.
3. The Respondent accepts and agrees to all terms and conditions, except changes as set forth in the response (refer to RFQ Attachment B, Item B#20), set out in the RFQ Attachment H, *pro forma* Contract.
4. The Respondent awarded the Contract resulting from this RFQ shall accept the State Purchasing Card ("P-Card") as a form of payment at no cost to the State.
5. The Respondent acknowledges and agrees that a contract resulting from the RFQ shall incorporate, by reference, all Respondent's responses as a part of the contract.
6. The Respondent will comply, as applicable, with:
   (a) the laws of the State of Tennessee;
   (b) Title VI of the federal Civil Rights Act of 1964;
   (c) Title IX of the federal Education Amendments Act of 1972;
   (d) the Equal Employment Opportunity Act and the regulations issued there under by the federal government; and,
   (e) the Americans with Disabilities Act of 1990 and the regulations issued there under by the federal government.
7. To the best of the undersigned's knowledge, information or belief, the information detailed within the Response to the RFQ is accurate.
8. The Response submitted to the RFQ was independently prepared, without collusion, and under penalty of perjury.
9. No amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Respondent in connection with the request or any potential resulting contract.
10. Both the Technical Response and the Cost Proposal submitted in response to the RFQ shall remain valid for at least 120 days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract pursuant to the RFQ.

By signature below, the signatory certifies legal authority to bind the responding entity to the provisions of this request and any contract awarded pursuant to it. The State may, at its sole discretion and at any time, require evidence documenting the signatory's authority to be personally bound or to legally bind the responding entity.
DO NOT SIGN THIS DOCUMENT IF YOU ARE NOT LEGALLY AUTHORIZED TO DO SO BY THE ENTITY RESPONDING TO THIS RFQ.

SIGNATURE & DATE: _____

PRINTED NAME & TITLE: _____

LEGAL ENTITY NAME: _____

FEIN or SSN: _____

REFERENCE QUESTIONNAIRE

The standard reference questionnaire provided on the following pages of this attachment MUST be completed by all individuals offering a reference for the Respondent.

The Respondent will be responsible for obtaining completed reference questionnaires as required (refer to RFQ Attachment B, General Qualifications & Experience Items, Item B.17.), and for enclosing the sealed reference envelopes within the Respondent's Technical Proposal.

RFQ # 32505-00215 REFERENCE QUESTIONNAIRE

RESPONDENT NAME: RESPONDENT NAME (completed by respondent before reference is requested)

The "respondent name" specified above, intends to submit a response to the State of Tennessee in response to the Request for Qualifications (RFQ) indicated. As a part of such response, the respondent must include a number of completed and sealed reference questionnaires (using this form).

Each individual responding to this reference questionnaire is asked to follow these instructions:

- complete this questionnaire (either using the form provided or an exact duplicate of this document);
- sign and date the completed questionnaire;
- seal the completed, signed, and dated questionnaire in a new standard #10 envelope;
- sign in ink across the sealed portion of the envelope; and
- return the sealed envelope containing the completed questionnaire directly to the respondent.

(1) What is the name of the individual, company, organization, or entity responding to this reference questionnaire?

(2) Please provide the following information about the individual completing this reference questionnaire on behalf of the above-named individual, company, organization, or entity.

NAME:	
TITLE:	
TELEPHONE #	
E-MAIL ADDRESS:	

(3) What goods or services do/did the vendor provide to your company or organization?

RFQ # 32505-00215 PROPOSAL REFERENCE QUESTIONNAIRE — PAGE 2

(4) What is the level of your overall satisfaction with the vendor of the goods or services described above?

Please respond by circling the appropriate number on the scale below.

	1	2	3	4	5	
least satisfied						**most satisfied**

If you circled 3 or less above, what could the vendor have done to improve that rating?

(5) If the goods or services that the vendor provided to your company or organization are completed, were the goods or services completed in compliance with the terms of the contract, on time, and within [insert something here]? If not, please explain.

(6) If the vendor is still providing goods or services to your company or organization, are these goods or services being provided in compliance with the terms of the contract, on time, and within [insert something here]? If not, please explain.

(7) How satisfied are you with the vendor's ability to perform based on your expectations and according to the contractual arrangements?

(8) In what areas of goods or service delivery do/did the vendor excel?

RFQ # 32505-00215 PROPOSAL REFERENCE QUESTIONNAIRE — PAGE 3

(9) In what areas of goods or service delivery do/did the vendor fall short?

(10) What is the level of your satisfaction with the vendor's project management structures, processes, and personnel?

Please respond by circling the appropriate number on the scale below.

	1	2	3	4	5	
least satisfied						**most satisfied**

What, if any, comments do you have regarding the score selected above?

(11) Considering the staff assigned by the vendor to deliver the goods or services described in response to question 3 above, how satisfied are you with the technical abilities, professionalism, and interpersonal skills of the individuals assigned?

Please respond by circling the appropriate number on the scale below.

	1	2	3	4	5	
least satisfied						**most satisfied**

What, if any, comments do you have regarding the score selected above?

(12) Would you contract again with the vendor for the same or similar goods or services?

RFQ # 32505-00215 PROPOSAL REFERENCE QUESTIONNAIRE — PAGE 4

Please add any additional comments to the response above.

REFERENCE SIGNATURE:
(by the individual completing this request for reference information)

_____
(must be the same as the signature across the envelope seal)

DATE:

_____

RFQ # 32505-00215 PRO FORMA CONTRACT

The *Pro Forma* contract detailed in following pages of this exhibit contains some “blanks” (signified by descriptions in capital letters) that will be completed with appropriate information in the final contract resulting from the RFQ.

***PRO FORMA* CONTRACT**

BETWEEN THE STATE OF TENNESSEE,
TENNESSEE DEPARTMENT OF AGRICULTURE
AND
CONTRACTOR NAME

This Contract, by and between the State of Tennessee, **Tennessee Department of Agriculture** ("State") and *Contractor Legal Entity Name* ("Contractor"), is for the provision of obtaining the software, implementation services, hosting and ongoing support the Consumer Industry Service Division's licensing, permitting, inspection, and education as further defined in the "SCOPE". State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is a/an Individual, For-Profit Corporation, Non-Profit Corporation, Special Purpose Corporation Or Association, Partnership, Joint Venture, Or Limited Liability Company.
Contractor Place of Incorporation or Organization: Location
Contractor Edison Registration ID # Number

A. SCOPE OF SERVICES:

A.1. The Contractor shall provide all service and deliverables as required, described, and detailed herein and shall meet all service and delivery timelines as specified by this Contract.

A.2. <u>Summary of Services.</u>

Through this contract, the State shall obtain an enterprise computer software system that shall : encompasses replacement of the current TDA regulatory system(s), including but not limited to comprehensive project management, business and system analysis, provision of package software, software customization, development of system interfaces, testing, training, system implementation, hosting, support, and maintenance.

Under the terms of this Contract, the Contractor shall develop the System to meet the requirements and to develop deliverables identified herein.

Appendix 1 – Glossary
Appendix 2 – Functional and Technical Requirements
Appendix 3 – Statistics
Appendix 4 – Reports
Appendix 5 – Forms
Appendix 6 – Contractor Requirements
Appendix 7 – State's Acceptable Use Policy and Acceptance Use Agreement
Appendix 8 – Non-disclosure Agreement (NDA)
Appendix 9 – Enterprise Information Security Policies
Appendix 10 – Deliverable Specification Sheet

The Contractor's responses to the appendices listed above shall bind the Contractor and become part of this Contract upon execution.

- The Contractor's obligations include: the Design, Development and Implementation (DDI) for the five project stages,
- The project includes hosting, support, and maintenance (HSM) during Stage 1, Stage 2, Stage 3, Stage 4, and Stage 5, followed by the 6-month warranty period after the approved implementation of Stage 5.
- Consecutive one-year hosting, support and maintenance periods, after the conclusion of the six-month retainage period at the TDA's discretion.

A.3. <u>Project Management.</u>

The State requires that the Contractor follow a systematic approach to the design, development, and implementation of the System to ensure that a comprehensive and expandable system is implemented. The State of Tennessee's Information Technology Project Management Methodology is Tennessee Business Solutions Methodology (TBSM). TBSM is based on the principles set forth by the Project Management Institute (PMI) and on industry best practices that are adapted to meet the state's needs. The table below provides a high level illustration of the TBSM project phases and activities included, but not limited to the standard project management templates, tasks and deliverables.

Tennessee Business Solutions Methodology

Pre-Engagement Phase	Project Initiation	Project Planning	Project Execution / Project Monitoring & Control	Project Closing
• Project Charter (initial draft) • Initial Project Assessment	• Project Charter • BA Approach • Requirements Mgmt Plan • BPI Plan • Process In , Diagrams & Desc Requirements Capabilities • Solution Approach	• Requirements Development Plan • Requirements Traceability Matrix • Project Mgmt Plan • Work Breakdown Structure • Activity List • Scope Statement	• Project Schedule • Risk Register • Status • Change Control • Communications • Training • Implementation	• Closing Documents • Project Evaluation • Lessons Learned

The Contractor will be required to utilize the TBSM model including the templates or a comparable project management methodology and accompanying template documents similar to the TBSM. In aligning with industry standards, The Tennessee Business Solutions Methodology (TBSM) encompasses many templates for use throughout the phases of project management.

The Contractor shall address all the Deliverables for the life-cycle phases in their project plan but can organize and plan for the accomplishment of the work based on their experience with projects of similar scale and scope. The complete TDA System detailed requirements, which identify the required functionality of the System, are provided in Contract Appendix 2 – Functional and Technical Requirements.

The Contractor shall define the overall Project Management approach for the project and should describe, in general terms, the roles and authorities of project team members from both the State staff and the Contract staff. The Project Management Approach should be based on the Contractors best practices and experience, and should be fully described in the section of the Project Management Plan. The Contractor confirms their commitment to meet all Project Management requirements resulting deliverables defined in this Section regardless of the approach proposed. Each subsection within the Contractor requirements provides a narrative on the requirements, followed by a table defining the tasks and Deliverables to be fulfilled by the Contractor.

The Contractor shall provide project Deliverables for the TDA System in the form and format agreed to by the State.

A.4. <u>Required Milestones</u>.

The implementation dates for the TDA system milestones are as follows:

TDA System Milestones	Description	Target Completion Date
Stage 1A	Those features and functions indicated in RFQ Attachment H - Appendix 2 as Stage 1A for the Food Safety, Petroleum, Weights & Measures programs	Go Live 03-1-16
Stage 1B	Those features and functions indicated in Appendix 2 as Stage 1B for the Food Safety, Dairy, Petroleum, Weights & Measures programs	Go Live 07-1-16
Stage 2	Ag Inputs - Feed, Seed, Fertilizer, Lime	Go Live 08-1-16
Stage 3	Plant Certification, Apiary	Go Live 10-1-16
Stage 4	Animal Health	Go Live 12-1-16
Stage 5	Pesticides	Go Live 02-1-17

A.5. Service Description.

The Contractor shall deliver the services and deliverables as described and detailed in *Pro Forma* Contract Appendix 6 — Contractor Requirements.

a. Kickoff Meeting and Presentation.

The Contractor shall participate in a State-led Kickoff Meeting. The purpose of the Kickoff Meeting shall be to introduce the Contractor to the State project stakeholders, and ensure agreement regarding project objectives, roles and responsibilities, strategy, and known risks. The contractor shall prepare and deliver a presentation for the kickoff meeting that synthesizes their approach to the overall project, provides high-level milestones, and introduces the Contractor team.

The Contractor Project Manager shall ensure timely and accurate submission of project management deliverables to the State Business Project Manager as listed below:

b. Project Initiation and Project Management Phase Requirements.

The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6, Tables 1 and 2.

Work Breakdown Structure (WBS) and Project Schedule lists the work packages to be performed for the project, and a schedule baseline that will be used as a reference point for managing project progress as it pertains to schedule and timeline

c. Weekly Status Report.

The Contractor shall prepare and submit to the State Business Project Manager a Weekly Status Report. The report shall contain a synopsis of the status of activities, outstanding issues and expected resolution dates, expended level of effort/burn rate, and key risks and issues. Items to be tracked in this report will include, at a minimum, open technical questions, requests for information, schedule of resources for the coming week, and requests for documentation.

The Contractor shall also report progress against the Project Schedule in the Weekly Status Report, including, at a minimum, an assessment of progress against plan, and details of slipping tasks. For any planned tasks that are not worked or completed during the reporting

period, the Contractor shall include an explanation of the failure to meet the schedule and detailed plans to overcome the failure and prevent its recurrence.

d. Monthly Progress Report.
The Contractor shall prepare and submit to the Project Steering Committee a Monthly Progress Report throughout the project's duration. Monthly Progress Reports shall contain, at a minimum:

i. Progress toward project milestones.
ii. Explanations of schedule and cost variances relative to the previous month's progress report and the baseline schedule and cost projections.
iii. Updates on implementation.
iv. Status of deliverables.
v. Action items and status.

e. Requirements Verification and Fit-Gap Analysis.
The Contractor shall work with State project team members, as identified by the State, to verify the requirements outlined in Contract Appendix 2 – Functional and Technical Requirements, and to map and document the extent that the Contractor's solution meets each requirement. The Contractor shall use its responses to Contract Appendix 2 – Functional and Technical Requirements, for the verification process. The Contractor shall document any necessary requirement changes or requirement gaps identified as a result of the requirements verification process.

f. Defect Tracking Log.
The Contractor shall develop and maintain a Defect Tracking Log which shall include at a minimum, for each Defect:

a. Unique tracking number.
b. Short name and description of the defect.
c. Reference to test condition that identified the defect.
d. Date Defect was identified.
e. Tester.
f. Disposition (e.g., Not a Defect, Fixed, Successfully Retested, etc.).
g. Severity Level.
h. Description of changes made to correct the defect.

g. Final Project Report.
The Contractor shall create a Final Project Report summarizing project activities, lessons learned, and recommended next steps. The Final Project Report shall be submitted to the State Business Project Manager no later than fifteen (15) business days prior to the Contract End Date. The State will provide written acceptance of the Final Project Report.

The Contractor shall prepare and deliver to the State for review and approval a Requirements Verification document that includes a finalized list of Business Requirements Specifications, which detail the specific features and functions of each requirement. The State will provide written acceptance of the Requirements Verification document.

Additionally, the Contractor shall provide other requirements as described in *Pro Forma* Contract, Appendix 6. An abbreviated listing of those items is detailed below.

a. Business Process Re-engineering.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 3.

b. Organizational Change Management.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 4.

c. System Design,
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 5.

d. System Development.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 6.

e. System Acceptance.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 7.

f. System Implementation.
The Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 8.

g. Training.
Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Tables 9 and 10.

h. Maintenance & Support.
Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 11.

i. System Support & Warranty.
Contractor shall work with the State Project Manager to develop all items identified in the *Pro Forma* Contract, Appendix 6 Table 12.

A.6. Business Process Re-engineering.
Certain State processes have been identified for re-engineering, based on the opportunity to achieve significant improvements, including:

- Manage, Process, and Track:
  - Applications, Permits & Renewal
  - Bill & Fee Collection
  - Inspection Management
  - Violation Tracking
  - Complaint Tracking
  - Mobile Access
  - System Common
  - Performance Data Analysis
  - Certification, Testing, and Training
  - System Use Training
- Ability of license process owners to easily design and create workflows within the System
- Customer service improvements (wait time reduction, better response to inquiries)
- Fraud reduction
- Efficiency and process cost reduction
- Customer web-based self-service
- Capturing and using the customer's e-mail and text addresses, using them to keep the customer up-to-date on the status of transactions, and reducing the number of customer service status calls to the State staff.
- Integration of content/document management services (i.e. accepting scanned customer documents at the State office or the customer's computer, attaching those documents to the State record, and using only the scanned images from that point forward.)

- Working closely with State applicants to initiate transactions through the web and eliminate paper in the process.
- Improved file search and reporting capabilities
- Integration with the State's e-payment service and State authorized payment card Vendor
- Interface with third-party entities

The Contractor shall create and deliver a full set of updated "To-Be" process flows that the Contractor recommends to modernize and streamline State license, permit, enforcement, training processes during the Design Stage.

A.7. State Project Team.

The State intends to commit needed internal resources in support of the successful and timely delivery of the System. During the Contract term, State staff will not report to Contractor staff, and Contractor staff shall not assign tasks to State staff. State staff will not be responsible for the completion of Contractor-assigned deliverables per this Contract. The State shall provide the following, in addition to other staff as needed.

a. State Project Manager.

The State Project Manager shall be the Contractor's point of contact for the Project. The State Project Manager shall be appointed and on-site at the State office on or before the Contract start date. The State Project Manager shall consult with the Project Steering Committee on a continuing basis in every stage of the Project. This joint effort shall ensure that the Project is properly implemented, supporting each program area's requirements, and properly documented. The State Project Manager shall provide expertise, assistance, and technical leadership in all Project matters, including but not limited to, policy, staffing and organization, environment, data, information processing, current systems, and acceptance testing. The State Project Manager shall work closely with the Contractor's Project Manager in day-to-day Project activities.

b. State Contract Administrator.

The State shall provide a Contract Manager who shall be responsible for ensuring that the Project is in compliance with the Contract and satisfies the State's requirements.

c. Other State Project Staff Assignments.

The State shall assign staff, according to the Project timeline, to key Project roles, as necessary, to participate with the Contractor's staff in all Project Management Processes and Project stages. At the State's discretion, State personnel may be substituted, added, or removed.

A.8. Contractor Project Team.

All employees of the Contractor, who shall perform Services under this contract, shall possess the necessary qualifications, training, licenses and permits as may be required within the contract.

a. Contractor's Key Project Staff.

Except as otherwise provided for herein, the Contractor agrees that the Key Project Staff (Project Manager, Business Analyst, Technical Manager/Lead, Lead Designer, Lead Trainer) will continue their assignment to completion of said assignment. The same individual may fill multiple roles.

The Contractors Project Manager shall be present on-site at critical points during the contract period and will be responsible for the day-to-day management of the project's timeline, personnel, and administration. The Project Manager's role shall include, but not be limited to, resource allocation, ensuring Contractor staff performance, ensuring the timely development, quality, and acceptance of implementation documents and all other Deliverables,

communicating with the Project Team, chairing the status meetings. The Contractor Project Manager will also be required, upon reasonable notice to meet with the State's Project Manager and other State and/or TDA executives when requested by the State's Project Manager. The Contractor's Project Manager shall always be able to be contacted through Final Acceptance of the TDA system

1. The Contractor understands that the confidence in the professional abilities of the State's approved Key Project Staff is a vital component to meet all requirements to successfully implement the TDA. Therefore, if the Contractor wishes to remove any of the approved Contractor's Key Project Staff from the project prior or after his or her commencement or during the assignment period, the Contractor shall first, before proceeding with such removal, consult with and seek the advice and opinion of the State Project Manager. If, after said consultation, it is mutually agreed that such a removal shall take place, the Contractor will promptly provide the resume of a recommended potential replacement having similar or better qualifications for the State Project Manager's review and approval. If the State Project Manager does not approve Contractor's recommended candidate, the Contractor will promptly provide additional candidates for the State Project Manager's review. If the State Project Manager still cannot agree to a replacement, the State Project Manager reserves the right to either (a) have Key Project Staff remain on the project, or (b) terminate this Contract for cause as indicated in *Pro Forma* Contract Section D.6. Upon State's Project Manager approval, the replacement will become Key project Staff and will be subject to the terms and condition of this Contract. If the Key Project Staff member's work has already commenced, the Contractor will ensure a smooth transition, including having the Contractor staff who is leaving train the replacement Contractor staff at the State's facilities (see Staff Transition Period below).

2. If the State Project Manager does not agree to the replacement of Key Project Staff and does not wish to terminate the Contract, the Key Project Staff member must remain on the Project and must continue to work with the same degree of professionalism he or she provided prior to the Contractor's request for removal. If the Key Project Staff fails to do so, or if the Contractor removes the Key Project Staff without the State Project Manager's consent, the State has the right to terminate as indicated in D.6 or assess liquidated damages as described in *Pro Forma* Contract Section A.30. - Performance Standards and Liquidated Damages. (Liquidated Damages).

b. Contractor Core Team.

The Contractor shall be responsible for and agrees to provide staff sufficient to complete the Project according to the Master Project Work Plan. In accordance with the Contractor's proposal, the Contractor shall submit a complete listing of the individuals on the Core Project team documenting their corresponding role(s) and an organizational structure diagram of the Project team. The initial Core Team and any subsequent substitution of Core Team members shall require approval by the State. Failure of the Contractor to provide a replacement with equal or greater qualifications within a reasonable time, not exceeding 30 days, may result in Contract termination. The Contractor shall be permitted to add or remove core team positions during the Post-Implementation Support Phase, as approved by the State.

c. Project Team Stability.

The Contractor understands that Contractor's staff turnover is detrimental to Project progress, the quality of the Deliverables and Services to be provided hereunder, and the skills transfer process. The State believes, therefore, that it is in its best interest to maintain the continuity of work assignments for all levels of Employees including, but not limited to the Key Project Staff. The State also recognizes that it can be difficult, or in some cases impractical to maintain said continuity. The Contractor agrees, therefore to make a good faith effort to minimize turnover of Employees it assigns to the Project. The Contractor further agrees that if the Contractor removes an employee who is Key Project Staff prior to completion of his or

her assignment, the Contractor will so notify the State's Project Manager, in writing, five (5) Business Days prior to said Employee's leave date. The Contractor will provide a replacement with similar or better qualifications. The Contractor will ensure that there is a smooth transition, including having the Employee who is leaving train the replacement Employee at the State's facilities.

Cessation of Work by Employees for Reasons beyond Contractor control:

1. Reasons beyond the control of the Contractor shall be defined as: (i) death of the Employee; (ii) new disability or illness; (iii) Employee resigns his or her position; (iv) termination for cause by the Contractor; or (v) any other reasons deemed acceptable by the State's Project Manager.

2. In the event that any Employee ceases work for the reasons specified in A.8.c.1, written notification must be forwarded to the State's Project Manager.

Staff Transition Period

In the event the Contractor initiates a staffing change identified as key personnel under this Contract or who has been onsite full time for a period of six (6) months or greater, and received the State Project Manger's approval as described herein, the Contractor will offer the State a mutually agreed upon transition period up to two (2) weeks. In such event the Contractor, at no cost to the State, shall furnish the State with the service of another Employee possessing the skills required for performance of the Service that would otherwise have been performed by the Employee seeking to replace. Replacement staff must have comparable or greater documented skills than the documented skills of the staff member being replaced. During the transition the departing staff and the new staff will work together to develop a transition plan to transition the responsibilities. The State reserves the right to approve this transition plan in writing.

Work Site and Schedule

The Contractor's team members who have been defined as full-time (100% of working time) within the Master Project Schedule (Contractors' Team), shall perform their duties on-site in Nashville, Tennessee, unless otherwise agreed to by the State in writing. Non full time Contractor staff is not required to be based in Nashville, TN, but shall be available to be on site during their active periods of project engagement, as reasonably requested by the State Project Manager. All team members working onsite shall be identified to the State, along with any Contractor issued equipment intended to be used on site.

The Contractor shall provide State with an advance monthly staff schedule no later than five (5) business days before the last day of the preceding month. Unless otherwise agreed to by both Parties, the Contractor Team will work a schedule on and off site as defined by the State's normal business hours. However, the State of TN holiday schedule and State employees work hours shall be considered for interdependent project tasks and assignments.

A.9. <u>State Provisions.</u>

The State shall provide workspace and internet access for each full-time Contractor personnel working at the project site.

A.10. <u>Deliverable Acceptance.</u>

Deliverables must meet all applicable State approved Acceptance Criteria developed in accordance with State Approved Acceptance Management Plans and Test Plans.

a. <u>Document Based Deliverables.</u>

For each document-based Deliverable other than status reports, the State shall have an acceptance period beginning on the date written Notification of completion was received from the Contractor and as outlined herein. All document-based Deliverables shall require the

written approval by the State Project Manager or his or her written designee that such Deliverables comply with the terms of the Contract.

The Contractor shall provide document-based Deliverables in the form and format agreed to by the State using deliverable specifications sheets approved by the Project Manager. The deliverable specification sheets will include, but not limited to the following information: Deliverable title, frequency, draft and final due dates, approval requirements, outline of contents, and delivery media. See Sample Contract Appendix 10 (Deliverable Specification Sheet).

1. The number of business days for any State initial review of a document-based Deliverable shall be no more than ten (10) Business Days, unless otherwise mutually agreed to in writing by the State Project Manager and the Contractors Project Manager in the Master Project Work Plan. The ten (10) Business Day period shall begin upon written transmittal by the Contractors Project Manager to the State Project Manager that the Deliverable is in final form and ready for approval, and shall be counted from and include the first Business Day following the delivery of the Deliverable to the State. The State shall provide the Contractor (a) with approval of the Deliverable or (b) with a written statement of the itemized deficiencies preventing approval.

2. The Contractor shall have ten (10) Business Days to complete all corrective actions or changes in order for such document-based Deliverable to conform in all material respects with the requirements set forth in the contract. The count of such Business Days shall begin on the first business Day following Contractor's receipt of the written statement of required corrective actions or changes.

3. If the State cannot approve the document based Deliverable after correction by Contractor, the Contractor's Project Manager and the State Project Manager may mutually agree to further steps to correct outstanding material deficiencies. However, in no event shall the total time allocated for review, correction and review of material deficiencies in a Deliverable, exceed thirty (30) business days.

4. The State will have final approval of all document-based Deliverables.

b. <u>Event Deliverables.</u>
For Event Deliverables the State's review process will include an acceptance process as detailed in the approved Acceptance Test Plan. The number of Business Days for any State initial review of an Event Deliverable shall be set forth in the Acceptance Test Plan. If there are multiple events that are part of a single Deliverable, the review process will take place after the final event. The State will determine whether the Deliverable conforms with the requirements set forth in the contract or documented prior to the event in the Acceptance Management Plan, and will approve or prescribe remedy actions for the Contractor consistent with that plan.

c. <u>Other Deliverables.</u>
For Deliverables that contain hardware or software programs, the State's Deliverable review process will include acceptance testing as detailed in an approved Acceptance Test Plan. The number of Business Days for any State initial review/test of a software-based Deliverable shall be set forth in the Acceptance Test Plan. The process for software Deliverables will be as follows. User Acceptance testing will take place in a test environment. After approval by the State, the software Deliverable will be migrated to the production environment. The software Deliverable will then be monitored according to the Production Verification process as described in Contract Appendix 6 (Contractor Requirements) – Table 8. The State will provide Deliverable Acceptance upon completion of Production Verification; the review period will reset starting on the date the State is notified that the correction has been made in the

production system. The State will have final approval of all hardware and software based Deliverables.

A.11. Change Orders.

The State may, at its' sole discretion and with written notice to the Contractor, request changes in the Scope that are necessary but were inadvertently unspecified in this Contract.

a. Change Order Creation.

After receipt of a written request for additional services from the State, the Contractor shall respond to the State, within a maximum of ten (10) business days, with a written proposal for completing the service. Contractor's proposal must specify:

1. the effect, if any, of implementing the requested change(s) on all other services required under this Contract;

2. the specific effort involved in completing the change(s);

3. the expected schedule for completing the change(s);

4. the maximum number of person hours required for the change(s); and

5. the maximum cost for the change(s) — this maximum cost shall in no instance exceed the product of the person hours required multiplied by the appropriate payment rate proposed for such work.

The Contractor shall not perform any additional service until the State has approved the proposal. If approved, the State will sign the proposal, and it shall constitute a Change Order between the Contract Parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this Contract.

b. Change Order Performance.

Subsequent to creation of a Change Order, the Contractor shall complete the required services. The State will be the sole judge of the acceptable completion of work and, upon such determination, shall provide the Contractor written approval.

c. Change Order Remuneration.

The State will remunerate the Contractor only for acceptable work. All acceptable work performed pursuant to an approved Change Order, without a formal amendment of this Contract, shall be remunerated in accordance with and further limited by Contract Section C.3.c., PROVIDED THAT, the State shall be liable to the Contractor only for the cost of the actual goods or services provided to complete the necessary work, not to exceed the maximum cost for the change detailed in the Change Order. In no instance shall the State be liable to the Contractor for any amount exceeding the maximum cost specified by the Change Order authorizing the goods or services. Upon State approval of the work, the Contractor shall invoice the State in accordance with the relevant provisions of this Contract.

A.12. Correction of Deficiencies.

Any corrections of deficiencies relating to the Contract Scope of Services requirements or deliverables and any investigation necessary to determine the source of such deficiencies shall be completed by the Contractor at no cost to the State.

A.13. Inspection and Acceptance.

The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or

performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

A.14. Workflow Business Rule Management.

The statutes, rules and regulations governing State licensing activities change frequently. A primary value proposition of this project is that as laws change and as agencies improve their licensing business processes, the System will enable these changes to be made quickly and easily by business process owners, not software developers. To achieve this objective, the System should be driven by a workflow engine, commonly called a Business Rules Management System (BRMS).

This system core should provide business rules authoring tool set to design, modify, test, deploy, and execute business rules separate from the application code. It should include a rules repository capable of tracking and reverting to older rule versions and tracking changes to rules based on the system user.

The system must provide the capability to guide a business process owner through the definition and creation of license workflows through a graphical user interface.

A.15. Reporting.

The System must generate a variety of reports that are based on the user, audience, and purpose of the report. Requirements range from standard formatted reports used on a routine basis to ad-hoc requests for specific information that is user defined. There will be a great need for a variety of ad-hoc and on-demand reporting of data. Among other things the solution must provide a foundation to standardize processes and information thus enabling management to make much more informed decisions. The success of the project in meeting this objective is tied to the ability for users to access and analyze this information through standard reporting tools.

The vision for reporting is to provide accurate, timely and relevant information to a broad base of information consumers; In this regard, access to licensing information (from the main data store) is essential. In addition, the data will serve as a platform to satisfy a broader scope of strategic informational needs. The reporting environment will be able to:

1. Provide a detailed level of statewide information that does not exist today;
2. Aggregate statewide Information and expand the ability to perform ad hoc queries;
3. Improve the data and methods available to the State staff; and
4. Provide this in an efficient manner, without negatively impacting the transaction processing environment.

It is expected that functionality available through the reporting environment will be enhanced over time and will likely evolve through stages that incrementally provide:

a. The proposed solution must enable the creation and management of the data reporting environment. This should include tools for:
(1). Extracting data from multiple operational databases and external sources;
(2). Cleansing, transforming and integrating this data; and
(3). Periodically refreshing the data to reflect updates at the sources if housed in other than the original sources.

b. Analysis and reporting is the ultimate goal of the reporting solution therefore the proposed solution must provide a robust easy to use set of front end tools to accomplish that goal. Basic elements of the front end toolset include:
(1). The ability to quickly construct both tabular and graphical ad-hoc reports.
(2). The ability to save and share reports with other users and groups.
(3). A choice of delivery methods and automatic scheduling options.
(4). A collection of predefined and customizable report templates and style sheets.
(5). Integration with standard desktop software and third-party reporting software; and
(6). Support for incremental enhancements to delivered functionality.

A.16. Organizational Change Management (OCM).

With the State transitioning from multiple internal and manual systems to new technology and business processes, job roles and organizational structures may be impacted. The Project's OCM resources should collaborate with the Agency's HR representative to determine the impact of these changes on the organization structure and job roles in the State.

This OCM collaboration should also focus on reducing resistance and increasing speedy adoption and productivity during and after the implementation of the future state. This should include, at minimum, an end user Communication Plan, a Training Plan and a comprehensive Change Initiatives Plan. The expected outcome of the OCM Strategy is to reach ultimate productivity and business results as quickly as possible.

A.17. Training Requirements.

The TDA will be a complex system that will be used daily by State staff. The State considers the training of these users to be critical for acceptance of the System as well as the daily use of the System. The System project team will review and approve all Contractor System training staff and user training materials, including training plans and role-based training materials.

The TDA project team training responsibilities include:

a. Review and approval of all role-based System training schedules.
b. Review and approval of all Contractor training staff.
c. Review and approval of the overall System training plan.
d. Identify all staff to be trained during the implementation by role.
e. Review and approval of all Contractor-developed role-based System training materials.
f. Provide training facilities, computers, and network connections for all of the System training sessions.
g. Designate a training environment for use during training.
h. Coordinate training activities with the State's Enterprise Learning Management System as appropriate.

The Contractor will train all applicable State staff and also provide State a "Train-the-Trainer" approach that will allow key State staff to acquire the knowledge of the System necessary to be able to deliver End-user Training. Additionally, the Contractor shall provide technical training for staff who will take over the administration of the System once in production.

A.18. Warranty of System Products/Services.

a. General Terms.

The Contractor expressly represents and warrants that the System, Work Product, software, deliverables, hosting, support, and maintenance and any other products or services resulting from the Contractor's services hereunder (including any such material produced pursuant to a change order) shall be compliant in all respects with the requirements of the Contract, the related RFQ, and, if applicable, any related change order, and represents and warrants that the System, Work Product, software, deliverables, support and maintenance and any other products or services will be free from errors, defects, deficiencies or deviations, and that the products or services will perform in such a manner as the Contract, related RFQ, change order require, so that the intended function of the System, Work Product, software, deliverables, and any other products or services is accomplished in all respects as intended by the Contract, the related RFQ, and, if applicable, any related change order, and is otherwise consistent with industry standards.

b. Retainage Period.

The retainage period shall be six (6) months, shall apply to the entire System and to products or services resulting from change orders and enhancements to the System, and shall begin on the following dates:

(1) The retainage period on the entire System begins with the date the Contractor completes the requirements of Implementation Stage 5 as set forth in RFQ *Pro Forma* Contract Appendix 6, Table 8, System Implementation Phase Requirements certifying full functionality of the System for the last Stage 5.

(2) If any change orders or enhancements are requested by the State subsequent to the implementation stage, the retainage begins on the date the State requesting the change order or enhancement provides written acceptance of the product or services resulting from a change order.

c. Warranty Coverage.

(1) The warranty encompasses any errors, defects, deficiencies or deviations discovered in any products or services, including third-party software used for the design and operation of the System even if the third-party software is not used in its ordinary and usual capacity.

(2) The warranty period begins at the State's sign-off and written acceptance of the Software Implementation.

(3) The warranty requires the correction by the Contractor of all products or services containing any errors, defects, deficiencies or deviations and any necessary modifications or revisions to products or services at no additional cost to the State, including, by example, and not by limitation, the design, coding, and operation of the System's software to perform any function required by the Contract and related RFQ, whether occurring in the original contract or resulting from a change order requested by the State, or which is procured in any amendment to the Contract, in any interfaces that are created, and in any training manuals and all system documentation provided by the Contractor.

d. Time Frames for Repair Services.

(1) The Contractor must promptly, at the direction of, and within the time specified, by the State, correct any errors, defects, deficiencies or deviations from specifications and all the Project-related ABENDS, recurring errors, and performance or operational delays.

(2) The Contractor shall provide emergency maintenance services to correct code problems or any performance or operational problems related to the design or coding of the system software, its functioning or interfaces on a twenty-four (24) hour, seven (7) days a week basis.

(3) The System, Work Product, deliverables, software or any other products and services, as applicable, shall be either replaced, revised, repaired or corrected within twenty-one (21) calendar days of written notification by the State of the errors, defects, deficiencies or deviations; provided, however, that if the continued use of a defective or deficient product or service would cause damage to the State system or associated data, or would otherwise seriously impair, as determined by the State, the ability of users of the system(s) to do their jobs or the functions for which the system was established, then the Contractor shall act to repair the deficiencies immediately, unless an extension is otherwise granted in writing by the State. Failure by the Contractor to act immediately shall trigger the damages set forth in Section A.30.

(4) The State will determine when any errors, defects, deficiencies or deviations requiring repair services have been resolved.

e. Resources Required for Repair Service.

The Contractor shall apply all necessary resources to correct the errors, defects, deficiencies or deviations and shall make these corrections within the time-frame specified by the State.

f. Contact for Repair Services.

(1) The Contractor will be the initial contact point for all defect notifications and support requests, regardless of the perceived source of the problem.

(2) The Contractor may elect to have telephone or on-site repair or support services performed by subcontracted personnel; however, if this is the case, the Contractor shall be responsible for coordinating the effort so that the use of any third-party support is transparent to the State and so that the State shall not have to deal directly with the subcontractor.

(3) The State reserves the right to approve subcontractors for defect remediation service, and the Contractor must obtain such approval the State in writing prior to the Contractor's election to use a Subcontractor.

g. Maintenance of Operations and Services During Corrective Action.

The correction of errors, defects, deficiencies or deviations in work products/services shall not detract from or interfere with software maintenance or operational tasks.

h. Sufficient Diligence.

The Contractor represents and warrants that, prior to entering into this Contract, it was provided with the opportunity to conduct all appropriate due diligence activities necessary or helpful in confirming that the Contractor had sufficient resources, technology, experience and access to information and assistance from the State to perform all services required by this Contract, including providing a fully implemented Stage 1a of the System suitable for the needs of by no later than March 1, 2016 and all remaining implementation stages no later than January 1, 2017 at a cost of no more than the amount set forth in its response to the RFQ.

i. Authority.

The Contractor represents and warrants that the Contractor is organized, validly existing, and in good standing under the laws of the state of its incorporation, that it has the legal and corporate power and authority to enter into the Contract and carry out its duties and obligations hereunder, that it has sufficient rights and authority to grant the licenses set forth in Section E.6 of this Contract, that the person executing this Contract on behalf of the Contractor has sufficient authority, by operation of law or corporate act, to bind the Contractor by his or her signature to all obligations herein, and that the use of the System in accordance with the terms of this Contract does not and shall not infringe upon, or constitute a misappropriation of, any patent, copyright, trademark, trade secret or other intellectual property or proprietary right of any third-party.

j. Laws and Regulatory Requirements.

The Contractor represents and warrants to the State that it shall perform all of its obligations hereunder in accordance with all applicable federal, state and local statutes, laws, rules, and regulations. The Contractor further represents and warrants to the State that the use of the System for its intended purpose shall comply with all applicable Regulatory Requirements. The Contractor further represents and warrants that it shall develop and provide modifications to the System (collectively, "Regulatory Modifications"), whenever such modifications are recommended, mandated or required to allow the State to comply with any Regulatory Requirements. The Contractor shall provide to the State fully tested Regulatory Modifications that are required to comply with any such Regulatory Requirements sufficiently in advance of the date on which the State is required to comply with any such Regulatory Requirements so as to enable the State to adequately test and implement such Regulatory Modifications. "Regulatory Requirements" means federal, state and/or local (in all localities in which the State conduct business) governmental and quasi-governmental statutes, regulatory requirements, ordinances, policies, edicts, rules, guidelines or standards related to the State and their authorized user's use of the System or the functions of the System.

k. Contractor Statements.
The Contractor represents and warrants that the System, hardware, and other materials sold or licensed under the Contract fully comply with all of the Contractor's statements and with all product demonstrations or other sales related exhibitions provided by the Contractor.

l. All Prerequisites Included.
The Contractor represents and warrants that the deliverables provided by the Contract, including any configurations indicated for those deliverables, include all material, including software and intellectual property, necessary for the State to use, maintain and/or modify the System independent of the Contractor or any third party. The Contractor further represents and warrants that its response to the RFQ identifies any software which is included in the deliverables and not licensed under Section E.6.b.(1) along with any restrictions on the activities which can be taken with respect to that software by the State.

m. Milestone Dates.
The Contractor represents and warrants that the Contractor is able to perform all of its obligations on or before the dates set forth in the Master Project Work Plan.

n. Services.
The Contractor represents and warrants that it shall perform, complete, and provide all services in conformance with the requirements in the Contract, related RFQ, and any applicable change orders in a good and workmanlike manner and in accordance with the highest comparable industry practices and standards that generally are applicable to services of a like kind; provided, however, that where this Contract specifies a particular standard or criteria for performance, this warranty is not intended to and does not diminish that standard or criteria for performance.

o. Pending Litigation.
The Contractor represents and warrants that it is not a party to any material pending litigation and knows of no threatened material litigation regarding its products or services, including the System, any deliverables required by this Contract, or any Contractor rights set forth in Section E.6.b.

p. Legal Privacy and Confidentiality.
Because the State will use the System to collect data and personal information about residents of certain U.S. states, the Contractor represents and warrants that (a) the System is as, or more, technologically secure as the highest comparable vendor security standards; and (b) upon request from any State, the Contractor shall provide a report comparing the security standards contained in the System and hardware to the then-current highest comparable security standards offered by other vendors.

q. Solvency.
The Contractor represents and warrants that it is financially solvent and any financial information provided to the State is true and correct.

A.19. System Performance and Availability.

a. Following a statewide implementation, the System shall be available continuously, as measured over the course of each calendar month period, an average of 99.9% of the time, excluding unavailability as the result of Exceptions as defined below (the "Availability Percentage"). "Available" means that the System shall be available for access and use by the State. For purposes of calculating the Availability Percentage, the following are "Exceptions" to the service level requirement, and the System shall not be considered un-Available if any inaccessibility is due to: (i) regularly scheduled downtime (which shall occur

only upon advance written notice during non-core business hours); or (ii) loss of the State's Internet connectivity.

Core business hours are defined as:

• 8:00 a.m. – 5:00 p.m. (CT) Mondays through Fridays, excluding State holidays.

Non-core business hours are defined as:
• 5:01 p.m. (CT) Friday – 7:59 a.m. (CT) Monday;
• 5:01 p.m. – 7:59 a.m. (CT) Monday through Friday evenings and selected State holidays;

Core business hours can be changed by the State. Scheduled downtime must be approved in writing in advance by the State.

b. System availability shall be provided at 99.9% availability in any given month, excluding times when the System is un-available as the result of an Exception (as set forth above).

c. The average System response time shall be no more than seven (7) to ten (10) seconds or less for online and web applications. Hourly intervals of monitoring shall be the expected measure. The response time measurement will be the amount of time from the application receiving a request until the user receives the result, i.e., internal application response time between receipt of a request and the requested page being downloaded to the user. The response time measurement shall not include the time required to transmit the user's request to the System.

d. Contractor must immediately notify the State if a standard SLA misses or is outside of variance. Notification must happen through telephone and/or email to customer-provided contacts and acknowledgment of the notification must be logged. The notification should be specific and detailed.

A.20. **Acceptable Use Policy and Acceptable Use Agreement.**
Contractor personnel who require a physical and/or logical presence (remote connection) within the State of Tennessee networked and/or physical environment must:

a. Ensure that all Contractor personnel maintain an awareness of and remain subject to the State of Tennessee Acceptable Use Policy. Contractor acceptance will be evidenced by the execution of agreements defined in the State's Acceptable Use Policy and User Agreement Acknowledgement. See Contract Appendix 7 for the State's Acceptable Use Policy and Acceptable Use Agreement.

b. A copy of the Tennessee Information Resources Architecture is identified in the State of Tennessee Enterprise Architecture document and will be provided upon request.

A.21. **Change Management & Go Live.**
The Contractor shall provide the following change management and go-live services:

a. The Contractor shall work with the State to develop change management and Go-Live strategies. These strategies should address but are not limited to the following:

1. Assessing the training needs of the user community.
2. Identifying the most effective format for training delivery.
3. Developing training deliverables.
4. Marketing the system and promoting user adoption.
5. Developing system documentation.

b. The Contractor shall work with the State to assess user training needs and develop training materials. Training materials should be sensitive to user roles (agency analyst, coordinator, executive), cover all system functionality, and be provided in an effective format. One format we would like to explore is screen capture video with voice over, and embedding such videos directly into the system for easy reference.

c. The Contractor shall work with the State to develop detailed system documentation. System documentation differs from training materials in that it defines the system architecture, explains project implementation activities, and demonstrates how the system can be tailored over time to fit evolving TDA needs.

d. The Contractor shall work with the State to and develop a change management implementation plan that culminates in system roll-out.

e. The Contractor shall work with the State to support Go-Live. This support task will be complete when system stability is achieved.

A.22. <u>Help Desk Support.</u>

The following section outlines the State's post Go Live help desk support requirements for the proposed system. The statements in this section are based on the proposed system "as delivered," meaning all software, configurations, and customizations delivered by the contractor during implementation. The contractor will provide the following help desk services after the system Go Live date. These services will be available to the system administrator(s) within:

a. The State prefers the following communication methods:

1. Phone (toll free for the State).
2. Email.
3. Remote System Access – Contractor ability to remotely login to the primary system interface to test functionality and collaborate inquiries.
4. Remote Server Console – The ability to remotely connect to sub-system server console(s) to troubleshoot and resolve issues.

b. Help desk staff will possess intimate knowledge of the delivered system and be capable of troubleshooting complex system issues to resolution. Staff must also be able to provide answers to complex questions. Staff skillset should be equivalent to help desk Tier 3 technical support.

c. Help desk calls will follow the procedure outlined below:

1. Call will be answered by Help Desk staff during hours outlined in A.67.
2. Help Desk staff will remotely connect to the proposed system to verify the issue described by the State.
3. A collaborative discussion will occur between the State and help desk staff to decide the nature of the call and assign call priority.
4. An email will be sent by the help desk to the State confirming the logged call details.
5. The identified issue will be resolved by the help desk within the time allotted by the table below.

A.23. <u>User Licensing.</u>

a. Contractor shall grants the State a perpetual, non-exclusive, transferable license for a minimum of 250 authorized users to all software necessary to access, run and use the system.

b. Contractor shall allow the State to increase the number of perpetual, non-exclusive, transferable licenses in increments of 10 for all software necessary to access, run and use the system.

c. By entering into this Contract, Contractor waives all terms and conditions contained in its order acknowledgement form, click or shrink wrap agreements, or other contracts or terms and conditions applicable to the Proposed Software which are different from or additional to the terms and conditions set forth in this Contract, and all such different or additional contracts or terms and conditions shall be null and void. The State's acceptance of any licenses granted by Contractor hereunder are expressly made conditioned on the parties' assent to the terms and conditions set forth in this Contract, and is limited to only a license for use of the Evaluated Software. Nothing in this Contract shall bind either party to accept any terms and conditions contained in this Contract for any subsequent contract or enter into a subsequent contract.

A.24. Architecture Management Plan.

The Contractor shall prepare and submit an Architecture Management Plan and shall keep the Architecture Management Plan current to reflect changes and current information. The Architecture Management Plan shall include all known tasks for managing and tracking the architecture activities for the duration of the Project, including the following:

a. A description of how quality attribute scenarios that are included in the *Pro Forma* Contract, Attachment H, will be integrated into the requirements baseline and managed from that point forward.

b. A description of how the technical management approach for ensuring that the System and software architecture descriptions are maintained as enduring "living documents" and accurately reflect all the approved System and software changes that have been subsequently approved and/or implemented since the architecture description was first placed under configuration management control.

c. A description of how the technical approach for implementing architecture compliance reviews required to be periodically conducted throughout the System life cycle, under State oversight. The objective of conducting these architecture compliance reviews (after the iterative design reviews have been completed) is to verify that the detailed design and software implementation complies with the approved System and software architecture baseline that is under configuration management control. As part of the approach, the Plan shall include a description of how often and when such architecture compliance reviews should be conducted to achieve the stated objective.

d. A description of the information the Contractor is going to collect, and report on, to track and manage all the architecture-related tasks described above.

A.25. Conduct Project Kick-off Meeting.

The Contractor shall conduct a Project "Kick-Off" Meeting with representatives of TDA to commence the Project. This meeting shall focus specifically on the responsibilities of the Contractor and working relationships and interactions among the Contractor and State staff, as set forth herein and shall include a review of the Master Project Work Plan. Presentation materials and handouts shall be developed by the Contractor and presented for review and approval, prior to the Project Kick-off Meeting. The Contractor shall provide attendees a written summary of the meeting immediately thereafter.

A.26. Project Steering Committee (PSC).

The PSC provides executive level guidance for the I Project. The PSC shall evaluate the Project at critical review points as defined by the State during the entire life cycle of the Project. The evaluation shall consider information from Project management and technical groups supporting

the Project such as database administration, technical systems support, and computer operations.

A.27. Narrative Project Status Report and PSC Presentation.
At a minimum, the Contractor shall make a semi-monthly presentation to the PSC. The narrative Project Status Report and presentation shall be provided that details the progress of the Project, identifies the monthly activities of the Project, documents upcoming key activities and identifies the issues and items needing PSC attention. The PSC may request unscheduled reports from the Contractor to address specific concerns relating to the Project status.

A.28. Intentionally left blank

A.29. Intentionally left blank

A.30. Performance Standards and Liquidated Damages.
The Contractor shall comply with minimum system and procedural performance requirements. At the first incident of failure to meet one or more of the defined performance standards, the State, in its independent discretion, may request a corrective action plan and establish an extension date by which the Contractor shall correct the deficiency. Continued failure to meet performance standards may result in imposition of the damages established in this paragraph or in the State deeming the Contract to be in breach.

The following table defines the standards required for Contractor performance for the Project and the associated liquidated damages, which the Contractor agrees to pay. The Contractor agrees that the amounts set forth in the table below represent a reasonable estimate of the damages that would occur from a breach, and that, due to the nature of the Contractor's obligations under this Contract, such amounts would be uncertain and not easily proven.

Performance Area	Performance Item	Performance Period	Liquidated and Additional Damages
Response time	The Project performance thresholds for application System response time as required by Section A.19.		One Thousand Dollars ($1,000.00) per day
Availability	The Project performance thresholds for application System availability as required by Section A.19.		Ten Thousand Dollars ($10,000.00) per day
Applications, Permits, and Renewals	Failure to issue TDA timely and accurate applications and permits which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from applicable go-live date.	$7,500 per day
	Failure to issue timely and accurate Renewal Notices for TDA licenses on the predetermined dates based on expiration period in which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	6 months from applicable go-live date.	$7,500 per day

Performance Area	Performance Item	Performance Period	Liquidated and Additional Damages
Bill and Fee Collection	Failure to accurately account for all monies assessed and collected through the Contractor system, which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from applicable go-live date.	$5,000 per day
	Failure to accurately and timely integrate with iNovah cashiering system, period in which failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from applicable go-live date.	$5,000 per day
	Failure to accurately generate a single consolidated invoice per Entity for all TDA assessed fees in which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date	$1,000 per day
Inspections	Failure to accurately capture inspection data and/or sample information on supported portable devices in a non-connected environment, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$1,000 per day
	Failure to generate accurate and timely Notices, Violations, and Inspection Reports, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$1,000 per day
	Failure to capture and associate uploaded attachments to inspection records, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$1,000 per day
On-Line Services	Failure to provide a secure user interface to which the Public may apply for and pay for multiple TDA Licenses via the internet, which the failure is solely due to the fault of the Contractor software, system configuration,	60 days from the applicable go-live date.	$2,000 per day

Performance Area	Performance Item	Performance Period	Liquidated and Additional Damages
	or due to Contractor action.		
	Failure to accurately and timely interface with the State Authorized Payment Card Vendor, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	60 days from the applicable go-live date.	$2,000 per day
System Performance	In a Severity Level 1 event as defined in A.67 Support, failure of the contractor to resolve the issue within the agreed upon service level agreement, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	30 days from the applicable go-live date	$2,000 per hour
	In a Severity Level 2 event as defined in A.67 Support, failure of the contractor to resolve the issue within the agreed upon service level agreement, which the failure is solely due to the fault of the Contractor software, system configuration, or due to Contractor action.	30 days from the applicable go-live date	$1,000 per hour

A.31. Right to Remove Individuals.
The State shall have the right at any time to require that the Contractor remove from interaction with State any Contractor representative who the State believes is detrimental to its working relationship with the service provider. The State shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the contract or future work orders without the State's consent.

A.32. Subcontractor Disclosure.
The Contractor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.

A.33. General.
The Contractor shall provide a Customized Solution - either Commercial Off-The-Shelf (COTS) Software OR Software Programs developed by the Contractor plus any other services or deliverables as required, described, and detailed herein that shall meet all service and delivery timelines as specified by this Contract. The solution must be housed in one or more of the Contractor's secure Data Centers or by a third party at one or more remote secure Data Centers that meet the requirements of this contract. The solution can be a cloud hosted SaaS (Software as a Service) solution. The State defines cloud hosted SaaS solution as an application offered to a user as a service. SaaS is a complete, turnkey application solution (that is, no IT organization-built solution is required). User access must be via a user-centric interface, such as a Web

browser. The Contractor shall use Web Services exclusively to interface with the State's data in near real time when possible.

A.34. Legal Compliance.

All System security shall be compliant with TN Enterprise Information Security Policies. The security policy is included in *Pro Forma* Contract Appendix 9 – Enterprise Information Security Policies.

Transmission/dissemination of all data must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."

The Contractor shall be compliant with PCI DSS v3, PCI PA-DSS v3, or other regulations that are relevant to this contract.

The Contractor will be responsible for review of existing Federal and State legislation, as well as guidance and other program or technical documentation. In addition the Contractor shall be responsible for review of existing documentation generated, maintained, or provided by the State, including initial requirements, process flows, policies, or other documentation. The Contractor shall be responsible for review of the State's current processes and system design. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

A.35. Reporting and Continuous Monitoring.

The contractor shall maintain a security management continuous monitoring environment that meets or exceeds the requirements in the Reporting and Continuous Monitoring, based upon the latest edition of SOC2 Type II, SOC3, or ISO27001 Cloud Computing Security Requirements Baseline and Continuous Monitoring Requirements. To safeguard against threats and hazards to the security, integrity, and confidentiality of any State data collected and stored by the Contractor, the Contractor shall afford the State access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the State as required by SOC2 Type II, SOC3, or ISO27001 security standards.

A.36. Miscellaneous Security Provisions.

The Contractor shall prepare and deliver a comprehensive written Security Plan describing how the System's application security features shall satisfy the security requirements found in this contract. The Plan shall include all recommended levels of security, limitations of capabilities, and any required rules, and shall incorporate any reasonable and lawful requests or requirements of the State. The format and content of security tables shall be included, as well as the recommended starting phase for establishing security profiles. Further, and without limitation, the Security Plan shall demonstrate how Contractor shall:

1. Protect all information and information systems in order to ensure:
   a. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information authenticity;
   b. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
   c. Availability, which means ensuring timely and reliable access to and use of information.

2. Secure the System and the information contained therein that connects to the State network, or any network operated by the Contractor, regardless of location.

3. Adopt and implement, at a minimum, the policies, procedures, controls, and standards of the States' Information Security Policies to ensure the integrity, confidentiality, and availability of information and information systems for which the Contractor is responsible under this contract or to which it may otherwise have access under this contract.

4. Conduct periodic and special vulnerability scans, and install software/hardware patches and upgrades to protect all automated information assets. These audits shall be performed by a third party qualified to perform such tests, including penetration tests of the internal and external user interface, annually. The Contractor must submit, for review and approval by the State, the proposed scope of testing as well as the name and qualifications of the party performing the tests. The Contractor is responsible for the costs of this testing. The State may elect to perform independent testing. The Contractor must address and resolve any application vulnerabilities as directed by the State. The Contractor must arrange for repeat testing to ensure that all identified vulnerabilities have been addressed as directed by the State.

5. Report the results of the scans described in no. 4, above, to the State on a monthly basis, with reports due 10 calendar days following the end of each reporting period.

The Contractor shall ensure that each user's role is based on the business functions they are required to perform. The State has the right to perform manual or automated audits, scans, reviews, or other inspections of the Contractor's IT environment being used to provide or facilitate services for the State. The State reserves the right to verify the infrastructure and security test results.

The Contractor shall not publish or disclose in any manner, without the State's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the State.

Access to State Data shall be limited to the Contractor's State-assigned employees. Staff with data access shall sign a nondisclosure agreement and a security agreement. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of State data, the Contractor shall afford the State access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

The Contractor shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Contractor. The State and the Contractor shall understand each other's roles and responsibilities.

The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own personal data.

Contractor must secure and encrypt all APIs and Open Interfaces.

No click through licenses or provisions will be allowed.

A.37. <u>Physical Security.</u>

All enterprise data processing facilities that process or store data shall have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference. Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel. Procedures for working in secure areas should be created and implemented. Access points such as delivery and loading areas and other

points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities. Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Secured cabinets or facilities should support further segregation based on role and responsibility.

Users should ensure that unattended data processing equipment has appropriate protection. All systems and devices owned and operated by or on behalf of the State should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The Contractor may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

A.38. Assessment of the System.

1. The contractor shall comply with requirements, including making available any documentation, physical access, and logical access needed to support this requirement. The contractor shall create, maintain and update logs and documentation according to certification standard controls.

2. Information systems must be reassessed by the State whenever there is a significant change to the system's security posture.

3. The State reserves the right to perform Penetration Testing. If the State exercises this right, the Contractor shall allow State employees (or designated third parties) to conduct Security Assessment activities to include control reviews. Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of State information for vulnerabilities.

4. The Contractor is responsible for mitigating all security risks found during Assessment and continuous monitoring activities. All high-risk vulnerabilities and moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The State will determine the risk rating of vulnerabilities.

The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the Standard State Desktop Configuration. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved configuration. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. Contractor shall provide all services requested through this Contract within the context of the technical environment described in *Tennessee Information Resources Architecture*.

A.39. Protection of Information.

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their own proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information. The State will retain unrestricted rights to State data. The State also maintains the right to request full copies of the data at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as Personally Identifiable Information (PII). This data shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure. The data must be available to the State upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the State..

A.40. Confidentiality and Non-Disclosure.

The State has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the State and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the State during and at the end of this contract. The contractor shall not release any information without the written consent of the State. Personnel working on any of the described tasks may, at State request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of State information and documents. Data will only be disclosed to authorized personnel on a Need-To-Know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. Any information made available to the Contractor by the State shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of State records. Each officer or employee of the Contractor to whom any State record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions.

A.41. Data Ownership.

The State will own all right, title and interest in its data that is related to the services provided by this contract. The Contractor shall not access State user accounts or State data except:

1. In the course of data center operations,
2. In response to service or technical issues,
3. As required by the express terms of this contract, or
4. At the State's written request.

All data obtained by the Contractor in the performance of this contract shall become and remain the property of the State.

Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of State information and comply with the following conditions:

1. At no time shall any data or processes that either belong to or are intended for the use of the State or its officers, agents or employees, be copied, disclosed or retained by the Contractor for subsequent use in any transaction that does not include the State.
2. The Contractor shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

A.42. Data Location.

The Contractor shall provide its services to the State and its end users solely from data centers in the United States of America. Storage of State data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store State data on

portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access State data remotely only as required to provide technical support solely within the U.S.

A.43. Encryption.
All data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the data. The Contractor shall ensure drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data. The solution should support 256 bit encryption or latest State standard. This provision also applies to the data-at-rest and data-in-transit protections provided by the solution, even if protection of data-at-rest and/or data-in-transit is implemented by external modules (rather than the solution itself). The State will hold all encryption keys.

A.44. Import and Export of Data.
The State shall have the ability to Import or export data piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the State to import or export data to or from other service providers.

A.45. Data Protection.
The Contractor represents and warrants that use of the System as contemplated hereunder including, without limitation, Work Product and any software, will not result in the loss, destruction, deletion or of data integrity issues of any State's data that is not easily retrievable or the alteration of any of State's data that is not easily reversed.

A.46. Payment Card Industry Data Security Standard (PCI DSS).
Payment Card Industry Data Security Standard (PCI DSS) v3 and PCI _PA-DSS v3) compliance is mandatory. Proof must be through an annual audit by a Qualified Security Assessor (a designation received from the Payment Card Industry Security Standards. (https://www.pcisecuritystandards.org/security standards)

A.47. Separation of Duties.
To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities.

Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible. The Contractor shall limit staff knowledge of State data to that which is absolutely necessary to perform job duties.

A.48. Security Incident and Data Breach.
The Contractor shall inform the State of any security incident or data breach. The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the State should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

The Contractor shall report any security incident to the appropriate State identified contact immediately. If the Contractor has actual knowledge of a confirmed data breach that affects the security of any State content that is subject to applicable data breach notification law, the Contractor shall

1. Promptly notify the appropriate State identified contact within 24 hours or sooner, unless shorter time is required by applicable law,

2. Take commercially reasonable measures to report perceived security incidents to address the data breach in a timely manner
3. Cooperate with the State as reasonably requested by the State to investigate and resolve the data breach,
4. Promptly implement necessary remedial measures, if necessary, and
5. Document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

Unless otherwise stipulated, if a data breach is a direct result of the Contractor breach of its contract obligation to encrypt personal data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law - all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

A.49. Access to Security Logs and Reports.

The Contractor shall provide reports to the State in a format as agreed to by both the Contractor and the State. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this contract.

A.50. User Registration, De-Registration, Provisioning and Access.

User access to information resources should be authorized and provisioned according to the Agency's employee provisioning process. Users should have the least privileges required to perform their roles as identified and approved by their agency. The allocation and use of privileged access rights should be restricted and controlled. A user's access rights should be reviewed validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies). All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day. All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in State managed data processing facilities or facilities operated on behalf of the State must use a multifactor VPN solution to obtain access.

Contractor must provide a Web interface in which an administrator can create, manage and delete user accounts. This interface will create sub-administrator accounts and configure IAM services. The Web interface must be supported for use in all major Web browsers. Contractor must support Security Assertion Markup Language (SAML).

The solution should support the ability to display the State Acceptable Use Policy (AUP) statement after unlocking the container on the device and ability to confirm acceptance.

A.51. Removable Media.

Removable media should be sanitized prior to removing it from the facilities for maintenance or repair. Removable media should be disposed of securely when no longer required, using approved State procedures. Removable media containing confidential information, confidential data, or sensitive data must be protected against unauthorized access, misuse or corruption during transport.

A.52. Change Control and Advance Notice.

The Contractor shall give advance notice to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

A.53. Security Certification, Accreditation, Audit.

At the State's request, the contractor shall provide proof of certification, accreditation, or audit on a yearly basis to the State to validate the hosting solution security. (Examples: SOC 2 Type II/ SOC 3, ISO 27001).

A.54. Malicious Code.

The Contractor shall represent and warrant that the Software, Application and Network shall be free from all computer viruses, worms, time-outs, other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the Software user's or another's software, hardware, networks, data or information. If the Contractor is aware of any security incident, vulnerability or other malicious code within their software or network the Contractor shall immediately disclose this information to the State via telephone and e-mail, as well as identify a timeline to mitigate and eliminate the risk.

A.55. System Interfaces.

The Contractor is required to exchange information between the State System and entities that are internal or external to the State. The discovery phase of the design process must include evaluation of the existing interfaces and specify modifications, enhancements, or replacements to the interfaces which must be integrated into the system. The Contractor shall develop interfaces that feature standardized data formats and characteristics as well as standardized methods of communication and data interchange where applicable. The Contractor must also provide data schema and mappings and a fully documented set of standard application interfaces to allow for future external data sharing.

The Contractor shall develop specification documentation for each interface incorporated into the State system during the Design Phase of this project. The Interface Specifications shall be non-proprietary and the property of the State. The State shall have full distribution rights to the interface specifications developed for the system. The system shall provide State staff the ability to select the method of interchange. Interfaces may be real time, batch or a combination of both.

RFQ Attachment H - *Pro Forma* - Appendix 2 – System Common contains a list of known system interfaces but does not constitute a comprehensive list of all needed interfaces that will be necessary for successful implementation. Some interfaces require encryption. The Contractor shall use encryption for data transfers. Protocols associated with specific interfaces shall be determined by the Contractor and approved by the State during design.

The Contractor must be able to integrate with the State's provider of Credit Card and Check Processing.

A.56. Content and Document Management Capability.

The System must incorporate content management capabilities. Content management is needed to manage and automate the publishing of licensing-related content via workflows. The System must incorporate document management capabilities. State employees and business entities have a need to provide documentation to satisfy licensing requirements. The System must offer the ability to upload, scan, store, index, archive, and retrieve these documents. A reportable audit trail must exist for each document, including upload, modified, accessed, deleted dates, and retention schedule-related actions.

The State wants the option to integrate their document management system with the System or to make use of document management available within the System.

Users must be able to upload electronic documents to the System as necessary at any point in a license application workflow. The documents must be associated with the applicant's profile, license application or any individual license transaction. Paper documents and forms must be submitted in some licensing processes. The System must accommodate scanning, storage and retrieval of these image files.

The system shall indicate that the required document has been scanned and maintain a link to the scanned image of all documents in the State's document management system. The system shall allow for electronic capture of customer's signature on any required documents.

The system shall allow for the viewing of all scanned documents. The contractor shall develop a Scanning Integration Design and obtain State approval of this design during the design phase of this project. The design shall show in detail how the system will integrate with the State's standard document management system and fulfill all of the requirements stated above. The printing of scanned images shall be limited to authorized state staff.

A.57. System Hardware.

All hardware will be hosted by the Contractor at either one or more of the Contractor's secure Data Centers or by a third party at one or more remote secure Data Centers. Each of these locations should meet the requirements of this contract.

The Contractor is responsible for providing all hardware needed to fulfill the requirements of the contract. The Contractor shall provide clear specifications of all hardware that is needed. The Contractor shall size the hardware to sufficiently meet the business need but not exceed what the State considers a reasonable amount of capacity. The Contractor shall deliver a Hardware Capacity Analysis and Growth Plan showing how the hardware requirements were derived and how to forecast additional hardware needs as system utilization and storage requirements increase. The State reserves the right to add change, reconfigure, consolidate or eliminate hardware at any time to meet the best interests of the State.

The Contractor represents and warrants that the System and specified hardware are fully compatible and interoperable with each other and with all third-party software and hardware products that the Contractor's marketing materials, product documentation, or RFQ references. In addition, Contractor shall provide all services requested through this Contract to be compatible with the technical environment described in the Tennessee Enterprise Technology Architecture Standard Products.

A.58. Environments.

The Contractor shall have four operating environments:

1. *Development* - Used for development of programmatic changes. Must be similar to production environment, but can be smaller in scale. This environment hosts the source code library, versioning/configuration management/release tools, and other software development and testing tools as needed.

2. *System Integration Test* - Used to verify new or modified code integrations with the current application baseline. Must accurately represent the production environment for the changes being tested, but does not require duplication of the entire production data set.

3. *Training* - A small scale mockup of the production environment, capable of representing the current production version or new versions soon to be implemented into production. This environment will be used to train users ongoing with real production data without making changes to the production database.

4. *Production* - The official system of record. In a cloud environment, the production environment shall provide sufficient elasticity to meet expected peaks in demand. Changes to the production environment are made only through documented change control procedures. The production environment shall be physically and logically isolated from the Development, System/Integration Test, and Training environments.

A.59. System Performance Monitoring and Tuning Utilities.

The system shall include all utilities for software performance monitoring and tuning. The Contractor shall be responsible for the performance monitoring and tuning activities of the system. The Contractor must perform regression testing on upgrades prior to installing or implementing the upgrades into production. For any new version or upgrade of the software, the Contractor must certify in writing to the State that all the previous capabilities still work in accordance with the contract requirements.

A.60. Intentionally left blank

A.61. Maintenance.

System Maintenance shall include all services necessary to maintain the system operational uptime and recovery from system failures. The Contractor must be proactively monitoring the system and not relying solely on the State to notify the Contractor of system problems.

The Contractor shall include a calendar of scheduled maintenance, which shall be updated, revised, and coordinated with the State quarterly, with all scheduled activities occurring within the maintenance periods set forth herein. Contractor shall not have more than 30 minutes of scheduled maintenance per month and must provide at least three business days of notice. The Contractor shall provide for infrastructure maintenance, upgrades, and enhancements over time. The Contractor shall include the following Infrastructure Maintenance services including, but not limited to:

1. Maintenance of all tiers from the infrastructure to the application;
2. Continuous performance monitoring;
3. Bug fixes, enhancements, including new features, functionality, and technology upgrades
4. Quality assurance and testing of modifications and upgrades;
5. All patch updates
6. Changes mandated by any state or federal statute or regulation;
7. Increases in data storage or transaction capacity;
8. Backup and restore;
9. Disaster recovery;
10. Sufficient networking bandwidth and hardware capacity to support the peak processing demands of the State;
11. Operational independence of the State; and.
12. Redundancy. The Contractor shall offer a fully redundant solution that will provide full business continuity.

A.62. Maintenance Log.

The Contractor shall keep a log of all maintenance technical support calls made to the help desk, technical maintenance and technical support personnel and document the complaints and problems reported to the help desk system by the State. The log shall be made available to the State as part of an electronic monthly reporting as well as any other time upon request by the State. The log must at a minimum contain the following information:

1. Date and Time of call;
2. Name of Caller;
3. Caller's Organization Name;
4. Caller's telephone number and/or email address;
5. Description of Reported Problem/Complaint;
6. Indication of whether the problem/compliant was resolved at time of call;
7. Description of any follow-up investigation/resolution plans;

8. Assigned Case number and
9. Date, Time and Description of Final Resolution.

A.63. Benchmark Tests.

To determine the growth and reliability of the System, the Contractor shall design and perform benchmark tests. The benchmark shall be designed to produce information that supports projections of system performance characteristics and capacity projections of the System under statewide operations for the contract life following the State's implementation. The benchmark shall also address stress tests at each level of technology employed by the System. A capacity simulation and benchmark report documenting the projections shall be submitted to the State for review and approval.

A.64. Capacity Planning.

The purpose of the Capacity Analysis and Evaluation Plan is to identify users and interfaces of the System and to assist State technical, operations, and telecommunications personnel in projecting the capacity requirements needed (disk space, memory, etc.) and communication requirements (bandwidth, lines, etc.) to support the System. The Contractor shall document the approach for the selection and utilization of computers and services (applications, communications, databases, gateways, firewalling, etc.) that provide a modular, scalable solution that meets the State's minimum performance objectives as defined below. The Contractor shall provide the planning coordination for the network to achieve the minimum performance standards required by the State and shall perform all System modifications required to ensure System performance meets the required performance standards. The Contractor's design and implementation solutions for capacity will be reviewed and evaluated during the Design and Development Phases as by the State. The approved capacity solutions involving hardware will become the minimal environment requirements.

The Contractor shall prepare interim and final Capacity Evaluation Reports which documents, in detail, the results of the tests and recommendations for resolving any problems, as outlined in the Capacity Analysis and Evaluation Plan. The Contractor shall provide detailed documentation demonstrating how the required response time shall be achieved by the application. A basis for all calculations and assumptions are to be shown. At a minimum, the documentation shall show line speeds, devices supported per circuit and per location, routing, average and peak traffic load, and average and worst case response times. The Contractor shall provide to the State all information about the impact of application solutions.

The Contractor shall provide written affirmation and validate that State's production environment shall support the Project in a full production capacity and meet performance standards. The Contractor shall conduct a Capacity Evaluation Test during the Development Phase of the Project that addresses the needs and performance measurements identified in the Capacity Analysis and Evaluation Plan. Capacity Evaluation Testing shall be performed at a system level by the Contractor and in cooperation with the State Project team during the development Phase of the Project. The Capacity Evaluation Test shall include a stringent stress test that includes a simulation of workload and volume testing for the State, which shall be used to test and monitor the limits of the System in a simulated production environment The Capacity Evaluation Test shall be performed at peak times with peak volumes. The Capacity Evaluation Test results shall determine whether the application conforms to acceptable response and hardware load conditions. The Contractor shall be required to perform capacity testing multiple times until satisfactory test results are obtained. The capacity test results shall confirm that the software and the hardware configuration meet the State's requirements.

The Contractor shall perform all application software, file structure, database, and system software modifications necessary to ensure system performance reaches acceptable levels in production environments, based upon the results of the benchmarks or the capacity simulation models. The Contractor shall work with the State's staff to make other modifications necessary to

ensure system performance reaches required performance standards in a production environment based on the results of system testing.

A.65. Scalability.
The Contractor represents and warrants that the System has the capacity to scale up to meet the States' processing load without requiring time to add infrastructure. This scaling must include scaling service up or down rapidly in terms of users, storage or network.

A.66. Storage.
Contractor will impose no limit to the State on the amount of storage utilized in the solution provided.

A.67. Support.
When the State staff calls the help desk/technical support, the Contractor's technical support staff should not place the State caller on hold for more than five (5) minutes.

The following table lists the State's Service Level Objectives. These Service Levels should serve as a guideline of the level of response and resources the State is seeking for all of the support periods. The Contractor shall propose Service Levels with these guidelines in mind.

Defect Severity Level 1 - Maximum Response Time Immediately and up to 2 hours after notification. Contractor will provide resources to fix until completed. Coverage will be provided 24 hours per day and 7 days per week. These are defined as urgent situations, when the State's system is down and the State is unable to use the system. A Level 1 Defect may have one or more of the following characteristics: (a) a critical function of the Application/Device is not available; (b) the Application/Device hangs indefinitely and/or causes other State applications to hang; (c) the Application/Device crashes and/or causes other State applications to crash; and/or (d) a security incident has occurred or is suspected to have occurred.

Defect Severity Level 2 - Maximum Response Time Immediately and up to 4 hours after notification. Contractor will provide resources to fix until completed. Coverage will be provided 24 hours per day and 7 days per week. These shall be defined as critical system component(s) that has significant outages and/or failure precluding its successful operation, or possibly endangering the State's environment. A Level 2 Defect may have one or more of the following characteristics: (a) the performance, functionality or usability of one or more of the Application/Device's parts is severely degraded; (b) multiple users are impacted; and/or (c) one or more business functions are unavailable or unusable by the end users. The system may operate, but is severely restricted. Failure causes a loss of function or data, but there is a mutually agreed upon workaround.

Defect Severity Level 3 - Maximum Response Time Immediately and up to 2 business days after notification. Contractor and State will agree to resources applied. Coverage will be provided from 8:00 a.m. to 6:00 p.m. CT weekdays [Excluding State Holidays]. These shall be defined as a failure of a system or part thereof which has a minor impact on a State business process and can be handled on a non-immediate basis. Examples may include user requests (e.g., a report is not formatted correctly) and peripheral problems (e.g., output fails to print properly).

Defect Severity Level 4 - Maximum Response Time as mutually agreed. Contractor and State will agree to resources applied. Coverage will be provided from 8:00 a.m. to 5:00 p.m. CT weekdays [Excluding State Holidays]. These shall be defined as cosmetic and minor errors; all the user tasks can still be accomplished. Example: Grammar errors, color changes, misspelled words, layout, etc.

The State reserves the right to determine and assign levels of severity for the issue/support problems.

The Contractors' technical support staff shall accept the call for assistance at the time the State places the initial call.

Contractor shall not close a Defect fix unless the fix has been demonstrated to either: (a) repair the functionality, performance and usability of the Application or Device to its pre-Defect level or (b) improve the functionality, performance and usability of the Application or Device from its pre-Defect level. Unless, for a particular defect, the State has provided prior written approval for different response times, the Contractor shall, for each calendar month and for each Severity Level, respond to one hundred percent (100%) of reported Defects within the Maximum Response Time during Hours and Days of Coverage agreed upon for each level of defect.

The State defines the problem resolution response time as the total elapsed time from when the Contractor's Help Desk has been contacted by the State and the system error/nonconformity severity level has been determined until the time when the issue or problem has been fixed, tested, and verified as being resolved as reasonably determined by the State in accordance with the aforementioned severity level provisions.

A.68. Termination or Suspension of Service.

In the event of a termination of the contract, the Contractor shall implement an orderly return of State data in a mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of State data. The State shall be entitled to any post-termination assistance generally made available with respect to the services.

During any period of service suspension or in the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase any State data for a period of 365 days after the effective date of suspension or termination.

After such period, the Contractor shall have no obligation to maintain or provide any State data.

When no longer required, information, data, and/or equipment will be returned to State control, destroyed, or held until otherwise directed at the State's discretion. Destruction of items shall be accomplished by following NIST Special Publication 800-88 or adherence to DoD 5220.22-M, Guidelines for Media Sanitization. Certificates of destruction shall be provided to the State.

A.69. Turnover/Transition Plan

The Contractor shall provide a Turnover/Transition Plan as part of this contract. Turnover is defined as those activities that are required for the Contractor to perform in order to transition contract operations to the State or a subsequent Contractor at the termination of the agreement. During the turnover the Contractor must ensure that program stakeholders do not experience any adverse impact from the transfer of services. The Contractor must fully cooperate with the State in achieving a smooth transition.

The Contractor shall create a Turnover/Transition Plan during the Initiation Phase and shall submit the Plan for approval by the State. The Contractor shall keep this plan current with any changes in subsequent phases. The Contractor shall outline its plan for turnover of the System from Contractor support to the support by the State. The Turnover/Transition Plan shall include the state of readiness required for System turnover, should it be required for transference or migration by the State, and shall outline the conditional criteria required to turn over responsibilities for the operation and support of the System from the Contractor staff to the State and the essential knowledge transfer to the State. The Contractor shall develop detailed specifications for describing States' staff responsibilities for System operations, support, and maintenance. The Turnover/Transition Plan shall describe all tasks to be performed by the State, and the Contractor to ensure a smooth transfer of services.

A.70. Notification of Legal Requests.

The Contractor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's data under this contract, or which, in any way might reasonably require access to the data of the State. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice.

A.71. Contract Audit.

The Contractor shall allow the state to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

A.72. Intentionally left blank

A.73. Disaster Recovery.

The Contractor will deliver thirty (30) calendar days before the system is implemented and maintain the plan throughout the life of the contract, a Business Continuity and Disaster Recovery (BC-DR) Plan, which is updated and tested at least annually and is subject to approval by the State. The plan must address recovery of business functions, business units, business processes, human resources, and the technology infrastructure.

The plan must ensure that the State's Recovery Point Objectives (RPO) of one hour and recovery time objective (RTO) of 4 hours are met. The Contractor shall continually review the Disaster Recovery Plan and make necessary updates to the plan at least annually to ensure the plan always contains accurate and up-to date information.

This plan shall include procedures for the periodic copying of data to other media and the process for restoring data to its original or prior form. The Contractor will be required to provide written evidence of this to the State. This evidence should be in the form of a detailed report describing the date tested, types of systems tested, outcome of tests, and any remedial items that testing may discover. Regardless of the architecture of its systems, the Contractor shall develop and be continually ready to invoke a business continuity and disaster recovery plan. The BC-DR plan shall encompass all information systems supporting this Contract. At a minimum the Contractor's BC-DR plan shall address the following scenarios:

1. Central and/or satellite data processing, telecommunications, print and mailing facilities and functions therein

2. System interruption or failure resulting from network, operating hardware, software, communications infrastructure or operational errors that compromise the integrity of transactions that are active in a live system at the time of the outage;

3. System interruption or failure resulting from network, operating hardware, software, communications infrastructure or operational errors that compromise the integrity of data maintained in a live or archival system; and

4. System interruption or failure resulting from network, operating hardware, software, communications infrastructure or operational errors that do not compromise the integrity of transactions or data maintained in a live or archival system but does prevent access to the system.

The Contractor shall periodically, but no less than annually, test its BC-DR plan through simulated disasters and lower level failures in order to demonstrate to the State that it can restore system functions. The Contractor shall submit an annual BC-DR Results Report to the State.

In the event that the Contractor fails to demonstrate in the tests of its BC-DR plan that it can restore system functions per the standards outlined in this Contract, the Contractor shall submit to the State a corrective action plan that describes how the failure will be resolved. The Contractor shall deliver the corrective action plan within ten (10) business days of the conclusion of the test.

In the event of a declared major failure or disaster, as defined in the Contractor's BC-DR plan, the Contractor's critical functionality, needed to perform the services under this contract, shall be restored within one hour of the failure's or disaster's occurrence. All State data shall remain within the continental United States of America.

The Contractor shall maintain a duplicate set of all records relating to this Program in electronic medium, usable by the State and the Contractor for the purpose of disaster recovery. Such duplicate records are to be stored at a secure fire, flood, and theft- protected facility located at least 25 miles away from the storage location of the originals. The Contractor shall update duplicate records, at a minimum, on a daily basis and shall retain said records for a period of one hundred and eighty (180) days from the date of creation.

A.74. Archiving.

The Contractor shall facilitate implementation of records management policies through a systematic archiving capability to meet requirements for statutory reporting and compliance. Archived information should be retrieved quickly and efficiently without adversely impacting performance and should fulfill public records retention and disposition requirements. Archived data must retain its historical business context.

A.75. Data and System Conversion.

All data in the scope of the required functionality, current and historical, from all existing State systems shall be converted from the existing systems into the new system. The existing license, permit, certification numbers must be maintained in the same size and format as the current license, permit or certification number.

All data being converted shall be “cleaned” prior to conversion, including but not limited to remediation of duplicated data, cleansing addresses and correcting known data errors. The Contractor shall manage the overall data cleansing process. The Contractor shall have sufficient logic in their conversion programs to detect and resolve data inconsistencies which can be resolved programmatically with a high level of confidence. For those data which cannot be reliably converted, the Contractor shall provide a report of those data, and provide a mechanism for recording corrections such that a) data which must be corrected by hand shall only require keying the changes, not the entire data value, and b) corrections shall be done in an orderly process which insures that all hand-correctable data is reviewed and corrected. The Contractor shall define specific data conversion algorithms at the applicable phase of the project for approval by State staff.

During the design phase, the contractor shall develop a Data Conversion Plan and obtain plan approval from the State. The plan shall describe data cleansing and conversion methods, identify the mapping of all data in scope to the new system, including all data transformations needed. The Conversion Plan ensures information integrity and the validity of the electronic content is maintained throughout the conversion and implementation phases. The Contractor shall work with the IT staff of the State to map data fields from each legacy system to the Contractor’s system, in preparation for the data conversion process. The Contractor shall provide data conversion rules for the State. The Contractor shall document data migration requirements and submit these requirements to the State for review and approval.

During the construction phase, the contractor shall develop and test data cleansing and conversion procedures (custom software programs, conversion tool configurations or scripts as needed). The contractor shall provide test results, control totals, record counts, etc., of the data before and after the conversion, and an audit of data before and after conversion for review and approval by the State.

During the implementation phase, the contractor shall provide data conversion results for State approval prior to implementation. The results shall include samples of converted data, control

totals, record counts, etc., of the data before and after the conversion, and an audit of data before and after conversion. During the implementation phase, all data shall be kept synchronized between the existing systems and the State system as necessary to keep implemented locations in synchronization with those not yet implemented. The Contractor shall perform functional, system, and integration testing to ensure all data was successfully converted and the system functions as expected after legacy data has been placed into the system. The Contractor shall correct all problems reported.

The Contractor shall convert electronic content from legacy systems that are being fully or partially replaced within the scope of the Project. The Contractor shall define the electronic content conversion process that will be used for each of these legacy systems. Integration testing shall be performed and results documented on this converted electronic content, prior to User Acceptance Testing. The plan shall address, at a minimum, the following to store its electronic content on the System's Electronic Content Repository:

1. Roles, responsibilities, and required staffing to support conversion.
2. Conversion overview noting objectives, approach, roles, techniques, testing process, electronic content validation, impact, and resources.
3. Conversion strategy for handling "black out" period when switching from the old system to the new and the interfaces associated with each.
4. Conversion process (automated manual, verification procedures, and acceptance responsibilities).
5. Identification of all electronic content sources.
6. Identification of electronic content and/or systems to be converted, replaced, or impacted.
7. Identification of electronic content needed to populate the System so that the Project is a fully functioning system.
8. Identification of all conversion tasks.
9. Schedule of conversion tasks.
10. Conversion environments.
11. Conversion support (system resource requirements, policy, and hardware).
12. Automated and manual conversion system activities.
13. Procedure for continually updating electronic content with additional/new electronic content from the source systems until all the Project sites have been implemented.
14. Identification of and planning for manual support requirements.
15. Identification of control procedures and evaluation criteria.
16. Special training for conversion activities.
17. Conversion testing.
18. Electronic content conversion and load process.
19. Identification and tracking of defects, error handling, and audit requirements.
20. Backup and recovery of converted electronic content, including disaster recovery requirements and methods for returning to State.
21. Procedure to review and compare the electronic content from each State's legacy system with the converted electronic content in the "To Be" System. These reviews shall be conducted, at a minimum, by functional area with any resulting discrepancies documented and fully explained for the approval of the State.
22. Inventory of electronic content from the legacy system that are successfully converted to those in the "To Be" System along with electronic content that cannot be converted. For electronic content that cannot be converted include a detailed explanation for review and approval by State.

A.76. <u>Develop Interfaces with State Solutions.</u>

The Contractor shall work with the State and other external entities to re-engineer and standardize interfaces with State internal and external systems to facilitate seamless integration with these systems.

The Contractor shall develop detailed Interface Design Specifications for all interfaces with the Project including, but not limited to, those defined in RFQ Attachment H - *Pro Forma* - Appendix 2

– System Common. For each Project interface, the Contractor shall identify interface files and processing limitations, define the operating environment, including architecture of the system and error control procedures. The Contractor shall ensure that the Project will integrate successfully all interface functionality. The Contractor is responsible for the design and development of interfaces including security and encryption of the data. The Contractor shall perform testing of all interfaces, in accordance with the Test Plans. This process often involves security access and passwords not available to the Contractor and may require coordination with external agency personnel whose systems shall interface with the Project. The Contractor must be able to integrate with the State's instance of Microsoft Exchange.

The Contractor must be able to integrate with the State's provider of Credit Card and Check Processing.

A.77. Create User Documentation.

The Contractor shall create user documentation for the Project in a format to be approved by the State. Electronic and hard copies of documentation shall be provided. The Contractor shall develop a User Manual that features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The User Manual shall be used by the State Acceptance Test team to mirror the production environment and verify manual content. The Contractor shall create user documentation for the Project in a format to be approved by the State. Electronic and hard copies of documentation shall be provided. The Contractor shall develop the Procedure Manual in a format to be determined by the State. The Contractor shall develop a Procedure Manual which features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The Procedure Manual shall document instructions for manual operations and tasks that are performed in direct conjunction with the automated system. It shall address each task performed in a step by step procedure that identifies the action (task to be performed) and the individual with responsibility to complete the action. The Procedure Manual shall be revised with any changes resulting from the State's Acceptance testing and initial user training sessions.

A.78 Warranty.

Contractor represents and warrants that throughout the Term of this Contract ("Warranty Period"), the goods or services provided under this Contract shall conform to the terms and conditions of this Contract. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.

Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, in conformity with standards generally accepted in Contractor's industry.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services.

A.79 Inspection and Acceptance.

The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

B. TERM OF CONTRACT:

B.1. This Contract shall be effective on September 30, 2015 ("Effective Date") and extend for a period of eighty-four (84) months after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

B.2. **Renewal Options.**
This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to three (3) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of one hundred twenty (120) months.

C. PAYMENT TERMS AND CONDITIONS:

C.1. **Maximum Liability.**
In no event shall the maximum liability of the State under this Contract exceed Written Dollar Amount ($Number) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

C.2. **Compensation Firm.**
The payment methodology in Section C.3 of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct or indirect costs incurred or to be incurred by the Contractor.

C.3. **Payment Methodology.**
The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.

a. The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

b. The Contractor shall be compensated based upon the following payment methodology:

The Contractor shall be compensated for said units, milestones, or increments of service based upon the following payment rates.

Total System Cost **This is the total from the RFQ Attachment E - Part-A of the Cost Proposal**		**$(NUMBER)**

The "Total System Cost" stated above shall be paid to the Contractor in installments contingent upon the completion of Project Phase Milestones, as follows:

PROJECT PHASE MILESTONE	**Percentage of Total System Cost to Be Paid**	**PAYMENT AMOUNT**
Project Initiation Phase and Project Management Requirements (Appendix 6, Tables 1 and 2)	5%	$[NUMBER]
Business Process Re-engineering, Organizational Change Management, and System Design Phase (Appendix 6, Tables 3 through 5)	5%	$[NUMBER]
Implementation Stage 1A (Appendix 6, Tables 6 through 10)	15%	$[NUMBER]
Implementation Stage 1B (Appendix 6, Tables 6 through 10)	15%	$[NUMBER]
Implementation Stage 2 (Appendix 6, Tables 6 through 10)	10%	$[NUMBER]
Implementation Stage 3 (Appendix 6, Tables 6 through 10)	10%	$[NUMBER]
Implementation Stage 4 (Appendix 6, Tables 6 through 10)	10%	$[NUMBER]
Implementation Stage 5 (Appendix 6, Tables 6 through 10)	10%	$[NUMBER
Retainage Period (6 Months post Stage 5 implementation – Appendix 6, Table 11)	20%	$[NUMBER]

Post Retainage								
	Year One	**Year Two**	**Year Three**	**Year Four**	**Year Five**	**Optional Year One**	**Optional Year Two**	**Optional Year Three**
Hosting, (includes 250 Licensed TDA Users)	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR	$ / YEAR
Support and Maintenance (Appendix 6, Table 11 through 12)	$ / YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR
User Licensing Fee for each additional 10 TDA users post retainage period. (*Pro Forma* Contract, Item A.23.b.)	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR	$ /YEAR

c. The Contractor shall be compensated for changes requested and performed pursuant to Contract Section A 11, without a formal amendment of this Contract based upon the payment rates detailed in the schedule below and as agreed pursuant to Section A 11, PROVIDED THAT compensation to the Contractor for such "change order" work shall not exceed SEVEN PERCENT (7%) of the sum of milestone payment rates detailed in Section C.3.b., above (which is the total cost for the milestones and associated deliverables set forth in Contract Sections A.3. through A.34. If, at any point during the Term, the State determines that the cost of necessary "change order" work would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	$ Amount (per compensable increment)
Project Manager	$ Amount /HOUR
Business Analyst	$ Amount /HOUR
Technical Manager/Lead	$ Amount /HOUR
Developer	$ Amount /HOUR
NOTE: The Contractor shall not be compensated for travel time to the primary location of service provision.	

d. Pro Rata Payments. A "day" shall be defined as a minimum of eight (8) hours of service. If the Contractor provides fewer than eight hours of service in a standard twenty-four hour day, the Contractor shall bill *pro rata* for only those portions of the day in which service was actually delivered. The Contractor shall not bill more than the daily rate even if the Contractor works more than eight hours in a day.

C.4. **Travel Compensation.**
The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.5. **Invoice Requirements.**
The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month and no later than thirty (30) days after goods or services have been provided to the following address:

State Agency Billing Address

a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

(1) Invoice number (assigned by the Contractor);
(2) Invoice date;
(3) Contract number (assigned by the State);
(4) Customer account name: State Agency & Division Name;
(5) Customer account number (assigned by the Contractor to the above-referenced Customer);
(6) Contractor name;
(7) Contractor Tennessee Edison registration ID number;
(8) Contractor contact for invoice questions (name, phone, or email);

(9) Contractor remittance address;
(10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
(11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
(12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
(13) Amount due for each compensable unit of good or service; and
(14) Total amount due for the invoice period.

b. Contractor's invoices shall:

(1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
(2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
(3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
(4) Include shipping or delivery charges only as authorized in this Contract.

c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. **Payment of Invoice.**
A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. **Invoice Reductions.**
The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

C.8. **Deductions.**
The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. **Prerequisite Documentation.** The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation. At the State's option, it may make payments to Contractor by automated clearing house ("ACH") or the State Purchasing Card ("P-Card").

a. The Contractor shall complete, sign, and present to the State:

(1) An "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and

(2) An "Authorization to Receive Payments by Purchasing Card Form" provided by the State. By doing so, the Contractor agrees that payments to the Contractor under this Contract may be made using the State P-Card.

b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

D. MANDATORY TERMS AND CONDITIONS:

D.1. Required Approvals.
The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

D.2. Communications and Contacts.
All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State: Tennessee Department of Agriculture

Name
Address
Email Address
Telephone # Number
FAX # Number

The Contractor:

Contractor Contact Name & Title
Contractor Name
Address
Email Address
Telephone # Number
FAX # Number

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

D.3. Modification and Amendment.
This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials. The State's exercise of a valid Renewal Option or Term Extension does not constitute an amendment so long as there are no other changes to the Contract's terms and conditions.

D.4. Subject to Funds Availability.
The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State

terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

D.5. Termination for Convenience.
The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

D.6. Termination for Cause.
If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity for breach of this Contract.

D.7. Assignment and Subcontracting.
The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.

D.8. Conflicts of Interest.
The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

D.9. Nondiscrimination.
The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

D.10. Prohibition of Illegal Immigrants.

The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment 1, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.

c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.

d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.

D.11. Records.

The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.

D.12. Monitoring.

The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.

D.13. Progress Reports.

The Contractor shall submit brief, periodic, progress reports to the State as requested.

D.14. Strict Performance.
Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.

D.15. Independent Contractor.
The Parties shall not act as employees, partners, joint ventures, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.

D.16 Patient Protection and Affordable Care Act.
The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.

D.17. Limitation of State's Liability.
The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.

D.18. Limitation of Contractor's Liability.
In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for intentional torts, criminal acts, fraudulent conduct, or omissions that result in personal injuries or death.

D.19. Hold Harmless.
The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Contract.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

D.20. HIPAA Compliance.

The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.

b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

D.21. Tennessee Consolidated Retirement System.

Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq*., the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

D.22. Insurance.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified below. The COI shall be provided ten (10) business days prior to the Effective Date and again upon renewal or replacement of coverages required by this Contract. If insurance expires during the Term, the State must receive a new COI at least thirty (30) calendar days prior to the insurance's expiration date. If the Contractor loses insurance coverage, does not renew coverage, or for any reason becomes uninsured during the Term, the Contractor shall notify the State immediately.

The COI shall be on a form approved by the Tennessee Department of Commerce and Insurance ("TDCI") and signed by an authorized representative of the insurer. The COI shall list each insurer's national association of insurance commissioners (also known as NAIC) number or federal employer identification number and list the State of Tennessee, Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 in the certificate holder section. At any time, the State may require the Contractor to provide a valid COI detailing

coverage description; insurance company; policy number; exceptions; exclusions; policy effective date; policy expiration date; limits of liability; and the name and address of insured. The Contractor's failure to maintain or submit evidence of insurance coverage is considered a material breach of this Contract.

If the Contractor desires to self-insure, then a COI will not be required to prove coverage. In place of the COI, the Contractor must provide a certificate of self-insurance or a letter on the Contractor's letterhead detailing its coverage, liability policy amounts, and proof of funds to reasonably cover such expenses. Compliance with Tenn. Code Ann. § 50-6-405 and the rules of the TDCI is required for the Contractor to self-insure workers' compensation.
All insurance companies must be: (a) acceptable to the State; (b) authorized by the TDCI to transact business in the State of Tennessee; and (c) rated A- VII or better by A. M. Best. The Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that the subcontractors are included under the Contractor's policy.

The Contractor agrees to name the State as an additional insured on any insurance policies with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) ("Professional Liability") insurance. Also, all policies shall contain an endorsement for a waiver of subrogation in favor of the State.

The deductible and any premiums are the Contractor's sole responsibility. Any deductible over fifty thousand dollars ($50,000) must be approved by the State. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.
The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

All coverage required shall be on a primary basis and noncontributory with any other insurance coverage or self-insurance carried by the State. The State reserves the right to amend or require additional endorsements, types of coverage, and higher or lower limits of coverage depending on the nature of the work. Purchases or contracts involving any hazardous activity or equipment, tenant, concessionaire and lease agreements, alcohol sales, cyber-liability risks, environmental risks, special motorized equipment, or property may require customized insurance requirements (e.g. umbrella liability insurance) in addition to the general requirements listed below.

The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability Insurance

1) The Contractor shall maintain commercial general liability insurance, which shall be written on an Insurance Services Office, Inc. (also known as ISO) occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises/operations, independent contractors, contractual liability, completed operations/products, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).

2) The Contractor shall maintain bodily injury/property damage with a combined single limit not less than one million dollars ($1,000,000) per occurrence and two

million dollars ($2,000,000) aggregate for bodily injury and property damage, including products and completed operations coverage with an aggregate limit of at least two million dollars ($2,000,000).

b. Workers' Compensation and Employer Liability Insurance

1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:

i. Workers' compensation and employer liability insurance in the amounts required by appropriate state statutes; or

ii. In an amount not less than one million dollars ($1,000,000) including employer liability of one million dollars ($1,000,000) per accident for bodily injury by accident, one million dollars ($1,000,000) policy limit by disease, and one million dollars ($1,000,000) per employee for bodily injury by disease.

2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:

i. The Contractor employees fewer than five (5) employees;

ii. The Contractor is a sole proprietor;

iii. The Contractor is in the construction business or trades with no employees;

iv. The Contractor is in the coal mining industry with no employees;

v. The Contractor is a state or local government; or

vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Professional Liability Insurance

1) Professional liability insurance shall be written on an occurrence basis. This coverage may be written on a claims-made basis but must include an extended reporting period or "tail coverage" of at least two (2) years after the Term;

2) Any professional liability insurance policy shall have a limit not less than one million dollars ($1,000,000) per claim and two million dollars ($2,000,000) in the aggregate; and

3) If the Contract involves the provision of services by medical professionals, a policy limit not less than two million ($2,000,000) per claim and three million dollars ($3,000,000) in the aggregate for medical malpractice insurance.

D.23. Tennessee Department of Revenue Registration.
The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.

D.24. Debarment and Suspension.
The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;

b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;

c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and

d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

D.25. Force Majeure.
"Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.

D.26. State and Federal Compliance.

The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.

D.27. Governing Law.
This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.

D.28. Entire Agreement.
This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.

D.29. Severability.
If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.

D.30. Headings.
Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.

D.31. Incorporation of Additional Documents.
Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:

a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;

b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below);

c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;

d. the State solicitation, as may be amended, requesting responses in competition for this Contract;

e. any technical specifications provided to proposers during the procurement process to award this Contract; and

f. the Contractor's response seeking this Contract.

E. SPECIAL TERMS AND CONDITIONS:

E.1. Conflicting Terms and Conditions.
Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. 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.

E.3. **Printing Authorization.**
The Contractor agrees that no publication coming within the jurisdiction of Tenn. Code Ann. §§ 12-7-101, et. seq., shall be printed pursuant to this Contract unless a printing authorization number has been obtained and affixed as required by Tenn. Code Ann. § 12-7-103 (d).

E.4. **State Ownership of Goods.**
The State shall have ownership, right, title, and interest in all goods provided by Contractor under this Contract including full rights to use the goods and transfer title in the goods to any third parties.

E.5. **Ownership of Software and Work Products.**

a. Definitions.

(1) "Contractor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.

(2) "Custom-Developed Application Software," shall mean customized application software developed by Contractor solely for State.

(3) "Rights Transfer Application Software," shall mean any pre-existing application software owned by Contractor or a third party, provided to State and to which Contractor will grant and assign, or will facilitate the granting and assignment of, all rights, including the source code, to State.

(4) "Third-Party Software," shall mean software not owned by the State or the Contractor.

(5) "Work Product," shall mean all deliverables exclusive of hardware, such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor exclusively for the State during the course of the project using State's money or resources, including Custom-Developed Application Software. If the deliverables under this Contract include Rights Transfer Application Software, the definition of Work Product shall also include such software. Work Product shall not include Contractor-Owned Software or Third-Party Software.

b. Rights and Title to the Software

(1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license granted under this Contract.

(2) All right, title and interest in and to the Work Product, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other

intellectual property and other proprietary rights embodied by and arising out of the Work Product, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Work Product, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Work Product. Contractor and its employees, agents, contractors or representatives shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties.

(3) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license granted under this Contract.

c. The Contractor may use for its own purposes the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of performing under this Contract. The Contractor may develop for itself, or for others, materials which are similar to or competitive with those that are produced under this Contract.

E.6. **State Furnished Property.**
The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible personal property furnished by the State for the Contractor's use under this Contract. Upon termination of this Contract, all property furnished by the State shall be returned to the State in the same condition as when received, less reasonable wear and tear. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the fair market value of the property at the time of loss.

E.7. **Work Papers Subject to Review.**
The Contractor shall make all audit, accounting, or financial analysis work papers, notes, and other documentation available for review by the Comptroller of the Treasury or his representatives, upon request, during normal working hours either while the analysis is in progress or subsequent to the completion of this Contract.

E.8. **Prohibited Advertising or Marketing.**
The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.

E.9. **Contractor Commitment to Diversity.**
The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to RFQ #32505-00215 (Attachment B, Item B.15) and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.

E.10. **Intellectual Property.**
The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor

notice of any such claim or suit and full right and opportunity to conduct the Contractor's own defense thereof, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

E.11. Liquidated Damages.

If an event, as described in *Pro Forma* Section A.30 occurs ("Liquidated Damages Event"), the State may assess damages on Contractor ("Liquidated Damages"). The State shall notify the Contractor of amounts to be assessed as Liquidated Damages. The Parties agree that due to the complicated nature of the Contractor's obligations under this Contract it would be difficult to specifically designate a monetary amount for Contractor's failure to fulfill its obligations regarding the Liquidated Damages Event as these amounts are likely to be uncertain and not easily proven. Contractor has carefully reviewed the Liquidated Damages contained in *Pro Forma* Section A.30 and agrees that these amounts represent a reasonable relationship between the amount and what might reasonably be expected in the event of a Liquidated Damages Event, and are a reasonable estimate of the damages that would occur from a Liquidated Damages Event. The Parties agree that the Liquidated Damages represent solely the damages and injuries sustained by the State in losing the benefit of the bargain with Contractor and do not include any injury or damage sustained by a third party. The Contractor agrees that the Liquidated Damages are in addition to any amounts Contractor may owe the State pursuant to the indemnity provision or any other sections of this Contract.

The State is not obligated to assess Liquidated Damages before availing itself of any other remedy. The State may choose to discontinue Liquidated Damages and avail itself of any other remedy available under this Contract or at law or equity.

E.12. Partial Takeover of Contract.

The State may, at its convenience and without cause, exercise a partial takeover of any service that the Contractor is obligated to perform under this Contract, including any service which is the subject of a subcontract between Contractor and a third party (a "Partial Takeover"). A Partial Takeover of this Contract by the State shall not be deemed a breach of contract. The Contractor shall be given at least thirty (30) days prior written notice of a Partial Takeover. The notice shall specify the areas of service the State will assume and the date the State will be assuming. The State's exercise of a Partial Takeover shall not alter the Contractor's other duties and responsibilities under this Contract. The State reserves the right to withhold from the Contractor any amounts the Contractor would have been paid but for the State's exercise of a Partial Takeover. The amounts shall be withheld effective as of the date the State exercises its right to a Partial Takeover. The State's exercise of its right to a Partial Takeover of this Contract shall not entitle the Contractor to any actual, general, special, incidental, consequential, or any other damages irrespective of any description or amount.

E.13. Unencumbered Personnel.

The Contractor shall not restrict its employees, agents, subcontractors or principals who perform services for the State under this Contract from performing the same or similar services for the State after the termination of this Contract, either as a State employee, an independent contractor, or an employee, agent, subcontractor or principal of another contractor with the State.

E.14. 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 and/or procure 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.

E.15. **Survival.**

The terms, provisions, representations, and warranties contained in this Contract which by their sense and context are intended to survive the performance and termination of this Contract, shall so survive the completion of performance and termination of this Contract.

IN WITNESS WHEREOF,
Contract Name:

CONTRACTOR SIGNATURE **DATE**

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

TENNESSEE DEPARTMENT OF AGRICULTURE:

JULIUS JOHNSON, COMMISSIONER **DATE**

***Pro Forma* ATTACHMENT 1**

(Fill out only by selected Contractor)

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	
FEDERAL EMPLOYER IDENTIFICATION NUMBER (or Social Security number)	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind Contractor. If said individual is not the chief executive or president, this document shall attach evidence showing the individual's authority to contractually bind Contractor.

PRINTED NAME AND TITLE OF SIGNATORY

DATE OF ATTESTATION

***Pro Forma* ATTACHMENT 2**

(Fill out only by selected Contractor)

SAMPLE LETTER OF DIVERSITY COMMITMENT

(Company Letterhead/Logo)

(Address)
(Date)
(Salutation),

(Company Name) is committed to achieving or surpassing a goal of (numeral) percent spend with certified diversity business enterprise firms on State of Tennessee contract # (Edison document #). Diversity businesses are defined as those that are owned by minority, women, small business and Tennessee service-disabled veterans which are certified by the Governor's Office of Diversity Business Enterprise (Go-DBE).

We confirm our commitment of (percentage) participation on the (Contract) by using the following diversity businesses:

(i) Name and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veteran) of anticipated diversity subcontractors and suppliers:
_____

(ii) Participation estimates (expressed as a percent of the total contract value to be dedicated to diversity subcontractors and suppliers):
_____%.

(iii) Description of anticipated services to be performed by diversity subcontractors and suppliers:

_____

_____

We accept that our commitment to diversity advances the State's efforts to expand opportunity of diversity businesses to do business with the State as contractors and sub-contractors.

Further, we commit to:

1. Using applicable reporting tools that allow the State to track and report purchases from businesses owned by minority, women, Tennessee service-disabled veterans and small business.

2. Reporting quarterly to the Go-DBE office the dollars spent with certified diversity businesses owned by minority, women, Tennessee service-disabled veterans and small business accomplished under contract # (Edison number).

(Company Name) is committed to working with the Go-DBE office to accomplish this goal.

Regards,

(Company authority – signature and title)

TERM	DEFINITION
Acceptance Criteria	The criteria defining the level of functionality and performance at which the deliverable/product and/or document need to perform/provide the State to consider the product/deliverable or part of the product complete. Acceptance Criteria will be defined in the greed upon Acceptance Management Plan.
Account Clerk	The cashier who receipts the monies received by the TDA.
Ag Inputs - Feed, Seed, Fertilizer, Lime	This program area regulates commercial animal feeds, commercial fertilizers, agricultural and vegetable seed and agricultural lime. This includes the issuance of permits or licenses, inspection of establishments, storage facilities, and manufacturing facilities, sample collection for laboratory testing, and fee collection for inspections or assessments. They also ensure compliance with the Federal Seed Act and federal laws regulating commercial feeds. Product labeling is reviewed and samples are obtained in the field. Samples are analyzed in house to ensure label guarantees are met and that standards of quality expected by the customer are achieved. This program area also administers the TN Commodity Indemnity Fund (CIF) that establishes a safety net for grain producers by creating an Indemnity Fund and requiring licensing, bushel assessments and sureties from commodity buyers.
Agency or Agencies	The State of Tennessee, acting by or through one or more departments, boards, commissions, offices or institutions of the State of Tennessee.
Alert	A flag which may be added to a license to indicate problems (i.e. disciplinary, payment), miscellaneous notes or an additional piece of information. The license alerts are displayed during related license maintenance and application processes.
Animal Health	This program area is responsible for the programs aimed at preventing, controlling and eradicating certain infectious or communicable diseases of livestock and other domestic animals. Activities include administering eradication programs for brucellosis, tuberculosis, scrapie, and pseudo rabies along with the control program for equine infectious anemia. Samples are collected and submitted for analysis and results are posted into the system. This program area provides oversight for the National Poultry Improvement Plan in Tennessee. This program area is also charged with the responsibility of enforcing laws and rules regulating interstate and intrastate movement of animals.
Apiary	This program ares is responsible for the recording of apiaries within the State of Tennessee by requiring that each apiary must be properly registered, with its' appropriate geographical coordinates. These coordinates are logged so that individuals and businesses within the State can notify apiary owners of their intent to spray pesticides, and so that they are only dispersed during hours in which the affected hives are dormant. This program area is also responsible for notifying apiary owners of the outbreak of American Foulbrood, a disease that affects apiaries,

TERM	DEFINITION
	and screening apiaries in close proximity to an outbreak to insure that they are not infected. This program area maintains a list of known individuals and businesses that assist in swarm removal and relocation.
Applicant	A person, individual, corporation, LLC, or partnership applying for a license or permit from the TDA.
Application	Submission of specified information and fees (if required), as a request for approval to conduct a regulated activity. License application is a general term that also applies to permits, certification, registrations, education and educational providers. Not all license applications lead to approval as they may not ultimately be approved by the regulating authority.
Application Fee	Monies required by the State in order to complete the processing of an Application.
Assistant Wizard	Help function/guide with external users of TDA system.
Authorized User	Any person(s) who has permission to use TDA and/or various functions pertaining to their specific job requirements
Barcode	An optical machine-readable representation of data, according to State standards.
Batch	Each cashier opens a batch every day in iNovah to receipt monies received by the TDA. Within the batch, every transaction is assigned a transaction number and a receipt number. The total dollar amount of all batches in an office each day should equal the total deposit for that date.
Business Rules	A rule of a business, company, or corporation. It is a rule that defines or constrains some aspect of business and always resolves to either true or false. Business rules are intended to assert business structure or to control or influence the behavior of the business.
Case	Usually related to Compliance functions. This is the identification, tracking, and resolution of a compliance matter and the data and actions associated with it. Examples are the handling and investigation of a complaint, or the investigation and prosecution of professional malpractice, or unlicensed practice.
Cash	Appropriate forms of payment would be a cashier's check, a money order, or a business check.
Cashier (Account Clerk)	The person who uses iNovah to receipt monies received by the TDA.
Central Procurement Office or CPO	The State of Tennessee Central Procurement Office (CPO).
Certification	A document confirming and/or validating a license history of a current or former license holder.
Check 21	The Check 21 Act took effect on October 28, 2004. The law allows the recipient of the original paper check to create a digital version of the original check, a process known as Check truncation, into an electronic format called a "substitute check", thereby eliminating the need for further handling of the physical document.
Complaint	A formal allegation of impropriety against an individual/entity.
Contract	The writing(s) which contain the agreement of the Central Procurement Office (CPO) and the Respondent/Contractor setting forth the total legal obligation between the parties as determined by

TERM	DEFINITION
	applicable rules of law.
Contract Requirements	The tasks and deliverables that the selected contractor will be responsible for once a contract has been executed and approved by the State.
Contractor	A firm that the State contracts with to provide services defined in the RFQ & Pro Forma Contract.
COTS Software Provider	A provider of commercial off the shelf Licensing and Enforcement software, a line-of-business (LOB) software product containing business rules and processes.
Customer	External users utilizing the TDA system to add, change, delete, or inquire. A customer can be a licensee, an applicant, a member of the general public, or other users of the system.
Dairy	This program area is responsible for the inspection of dairy farms, dairy plants, milk transport trucks, dairy and trade product distributors and milk samplers. Samples are collected and specialized laboratory analyses are performed and results are reported. The Contractor shall design the System to integrate with the State's existing system so that sample results will be tied directly back to the inspected facility. A mechanism for integrating data from outside (private) laboratories must also be provided for by the Contractor.
DBA	Doing Business As. This is your trade name.
DBA Change	A business may request to change their "Doing Business As" name, or trade name. Documentation must be submitted and approved prior to any actual change. The license number and expiration date do not change.
Defect	A failure of a configuration, modification, and/or customization of the software to operate in accordance with the Acceptance Criteria or RFQ functional or technical requirements or a failure of the Software to operate in accordance with the Software program documentation.
Deliverable	Any document deliverable, software deliverable or service that the Contractor is required to provide the State under the Contract.
Deliverable Acceptance	The written approval by the State Project Manager or his or her written designee that one or more Deliverables have met all applicable Acceptance Criteria and comply with the terms of the Contract.
Documentation	Refers to various types of document that will have to be prepared by the contractor and provided to the State in a form and format specified by the State. Types of documentation include, but are not limited to, pre and post meeting documentation, system documentation, technical documentation, training documents etc.
Downtime	The period of time in a given month when the System, or any portion thereof, because of failure of any or all software, is not operation in conformance with the defined System Requirements. Down-time shall begin 15 minutes after the Contractor is notified of the issue.
ERP	Enterprise Resource Planning is the State's Edison system. The new system will need to interface with Edison financials for cashiering purposes.
Edison	The State's Enterprise Resource Planning System.
Entity	An individual, group of individuals, business, brand, product or

TERM	DEFINITION
	object that has a unique identity. The applicant that applies for or holds a license or permit. Entity could be an LLC, Corporation, partnership, sole proprietorship etc.
Expiration	When the time period for an issued license or permit is over.
External Miscellaneous Transaction	A licensee, an applicant, a member of the public or any other user of the system who submits and application via the Internet which upon approval, will perform an action and/or amend information related to a specific entity and/or associate license.
External User	Synonymous with customer - a licensee, an application, a member of the general public or other users of the system.
Fees	Costs or payments related to licensing, e.g.: application fees, license/permit fees, renewal fees, education fees, and processing fees.
Final Acceptance	The point in the lifecycle at which the System Implementation is complete for all phases of the system and TDA agrees that the production system has performed for a pre-defined period (Software Production Verification) according to all Acceptance Criteria and System Requirements in the production environment.
Fine	In any case where the TDA is given the power to suspend or revoke any license or permit, they can levy a fine to remedy the matter. Fines are dollar amounts assigned by citations for violations of the rules and regulations or Tennessee Code Annotated.
FIS	Fidelity National Information Services, Inc. is the provider of banking and payments technology for the State of Tennessee. The payments-focused platforms will be used in supporting the State's benefits programs and payment collections. FIS enables the State to easily accept payments for recurring services, such as public utilities, or for one-time fees, fines and citations.
Fiscal Year	The TDA operates on a fiscal year from July 1 through June 30.
Flag	This term is synonymous with alerts and notifications and can have a number of different types which based on the type would trigger a workflow process.
Food Safety	This program area is also responsible for assuring the public of a safe, wholesome and properly represented food supply through permitting and inspection of food establishments, inspection of food products, and performance of specialized laboratory analyses on a variety of food products sold or produced in the State. This program area inspects food manufacturers, food warehouses, and food distributors to ensure wholesome food processing and storage practices. Samples are collected and specialized laboratory analyses are performed and results reported through an external system. Sample results will be tied directly back to the inspected facility. Tobacco Compliance is responsible for inspections that are conducted in retail establishments to ensure compliance with Tennessee statutes prohibiting the sale of tobacco products to persons less than eighteen years of age. Underage youth accompanied by an adult, visit stores and attempt to purchase a tobacco product. Proper packaging and signage are verified. Merchants are notified of the outcome and civil penalties are issued for second or subsequent violations.

TERM	DEFINITION
Food service establishment	(A) Food service establishment means any establishment, place or location, whether permanent, temporary, seasonal, or itinerant, where food is prepared and the public is offered to be served or is served food, including, but not limited to, foods, vegetables, or beverages not in an original package or container, food and beverages dispensed at soda fountains and delicatessens, sliced watermelon, ice balls, or water mixtures; (B) Food service establishment includes places identified in subdivision (A), regardless of whether there is a charge for the food; (C) Food service establishment does not include private homes where food is prepared or served and not offered for sale, retail food store operations other than delicatessens, the location of vending machines or supply vehicles; (D) Food service establishment does not include churches, temples, synagogues or other religious institutions, civic, fraternal, or veteran's organizations where food is prepared, served, transported, or stored by volunteer personnel only on non-consecutive days; provided, however, that the storage of unopened, commercially canned food, packaged bulk food that is not potentially hazardous as defined by department rules and regulations, and dry goods shall not apply for these purposes; (E) Food service establishment does not include grocery stores that may, incidentally, make infrequent casual sales of uncooked foods for consumption on the premises, or any establishment whose primary business is other than food service that may, incidentally, make infrequent casual sales of coffee or prepackaged foods or both, for consumption on the premises. For the purposes of this subdivision (9)(E), infrequent casual sales means sales not in excess of one hundred fifty dollars ($150) per day on any particular day; (F) Food service establishment does not include a location from which casual, occasional food sales are conducted solely in connection with youth-related amateur athletic or recreational activities or primary or secondary school-related clubs by volunteer personnel and that are in operation for twenty-four (24) consecutive hours or less; (G) Food service establishment does not include a catering business that employs no regular, full-time employees, the food preparation for such business is solely performed within the confines of the principal residence of the proprietor, and the catering business makes only occasional sales during any thirty-day period; and (H) Food service establishment does not include a house or other residential structure where seriously ill or injured children and their families are provided temporary accommodations in proximity to their treatment hospitals and where food is prepared, served, transported or stored by volunteer personnel; provided, that the

TERM	DEFINITION
	house or structure is supported by a 501(c)(3) organization, as defined in 26 U.S.C. 501(c)(3), that has as a component of its mission the support of programs that directly improve the health and well-being of children;
GIS	Geographic Information System.
International Standards Organization	ISO27001 ▪ An internationally recognized structured methodology dedicated to information security. ▪ A management process to evaluate, implement and maintain an information security management system. ▪ A comprehensive set of controls comprised of best practices in information security. ▪ Applicable to all industry sectors. ▪ Emphasis on prevention.
iNovah	The cashiering system utilized by the State of Tennessee. Each transaction is numbered and assigned a specific receipt number, and transactions each day are grouped into a batch for each cashier. Batches are dated the day they are to be deposited, and the total of all batches in an office should equal the total of that day's deposit for each office, as well as the total on the mail log.
Inspections	An inspection will be conducted by a TDA agent after a new application has been reviewed by the TDA office. The agent will bring a copy of the rules and regulations. They will also verify that the establishment meets the qualifications of the type of permit applied for, and in some cases determine the required license fee. Renewal inspections are done prior to the expiration of a license, and routine inspections can be done periodically during the license term.
Internal User	Users of the licensing system who work for a state agency participating in the licensing project. These users generally process, review or manage information provided by license applicants or other non- state people who use the system (external users).
License	The TDA issues several licenses to qualified applicants. The license must be prominently posted in a conspicuous location in your licensed establishment.
License Application	Submission of specified information and fees (if required), as a request for approval to conduct a regulated activity. License application is a general term that also applies to permits, certifications and registrations as well as licenses. Not all license applications lead to the approval and granting of a license, permit, certification or registration as they may not ultimately be approved by the regulating authority.
License Fee	Also referred to as a privilege tax.
License Status	The state of a license at a particular time, noted such as current, cancelled, expired, null and void, suspended, revoked, etc.
Licensee	Any establishment that holds a license from the TDA.
Mail Log	Any mail, Fed Ex, UPS, or other incoming type of mail that includes any form of money must be opened with two individuals present, and logged into a mail log which notes who it applies to, when it was received, and what check number is on a check or money

TERM	DEFINITION
	order.
Mandatory Requirements	Requirements that the Respondent must meet in order to be eligible for contract award
Miscellaneous Transaction	A transaction which performs and action and/or amends data for a specific entity and/or associated license. These transactions may be "one off" transactions as defined by business rules.
Monthly Report	At the end of each month, each office compiles a report of all licenses issued and voided during that month.
Notification	An official announcement about an action that has been taken or will be taken relating to a license record or business process.
Payment Card Industry	The Payment Card Industry Data Security Standard (PCI DSS) was created by the major credit card issuers, and applies to companies that accept, store process and transmit credit cardholder data. When it comes to data center operators, they should prove they have a PCI compliant environment with an independent audit.
Pesticides	This program area regulates the use, misuse, distribution and sale of pesticides across the state. This includes the issuance of certificates (i.e., Commercial and Private applicator certifications, licenses, charter companies, restricted use product dealers, and Worker/Handler), registration of all pesticide products sold in the state, conducting inspections of Pest Control companies, investigating complaints regarding pesticide related health and/or environmental issues, and ensuring compliance with Federal Groundwater, Endangered Species and Worker Protection Acts. The Pesticide section is also responsible for administering the licensing examinations, approves industry sponsored training and applies CEUs to records for all of those applicators who hold a current certification in the state.
Permit	Permits are generally issued to individuals or business. The individual holder of the permit is responsible for renewal of a permit prior to the expiration of that permit and the permit is the sole property of such individual holder. There is no grace period for an expiring permit.
Permit Term	The length of time that a license is current and valid.
Petroleum	This program area monitors the quality of petroleum products conveyed for commercial consumption in Tennessee. Commercial facilities are inspected annually for compliance with applicable laws and regulations. Inspections include water bottoms in storage tanks, dispenser labeling requirements, and field tests such as gasoline octane and diesel fuel flash point. In addition, samples of the product are collected and sent to a central laboratory for extensive analysis. All inspection and laboratory results are entered into a computer system and are linked to the establishment where they are collected.
Plan view	The State's Enterprise Portfolio Management tool.
Plant Certification	This program area is responsible for the inspection and certification of all firms in Tennessee dealing in production and sales of rooted plant materials. All nurseries are required to be inspected a minimum of once a year and greenhouses are inspected twice a year. Retail sellers of plant materials are audited once every three years. Other functions include special inspections for various compliance agreements and issuance of Phytosanitary Certificates (Both Federal & State). Certificate holders are subject to civil penalties for violating the Plant Pest Act and any of it associated

TERM	DEFINITION
	rules. Charges for requested Nematode samples occur for nurseries that ship to various countries. These products are inspected for proper labeling and sampled / analyzed to ensure products are as represented by product label and meet standards set by state or federal requirements.
Program Area	A Program Area consists of a set of operational activities under the general supervision of a Program Administrator. The Consumer and Industry Services Division is comprised of the following Program Areas: Ag Inputs, Animal Health, Apiary, Dairy Inspection, Food Safety, Pesticide Services, Petroleum, Plant Certification, and Weights & Measures.
Prominent	Standing out so as to be seen easily; particularly noticeable.
Policy and Procedures	The manual to provide guidance for internal regulations and procedures for TDA employees.
Renewal Inspection	Prior to the expiration of a license, a TDA inspector will conduct a renewal inspection at the place of business. He will either leave the paperwork for the renewal, or direct them to the forms online that they need to submit. The inspector will verify that the establishment continues to meet the legal requirements of their license and the amount of their renewal license fee. He also checks for the proper, unexpired employee permits and verifies that all signs and licenses are properly posted.
Renewals	Licenses are issued to expire based on business rules from the date of issue, or on a calendar year for certain types of licenses. Before a license expires, if an establishment wishes to keep their license, they must submit a renewal application to the TDA along with any required supporting documents and the renewal license fee. A license cannot be renewed until all documents are submitted, all citations are paid, and any outstanding issues are remedied.
Replacement Card	If an individual loses their employee permit, they can apply to the TDA for a replacement permit by submitting the appropriate form, either online, or through the mail.
Respondent	The entity that submits materials to the State in accordance with these instructions.
Response	The material submitted by the respondent in answering the solicitation.
Responsible Bidder or Responsible Respondent	A Bidder that is determined to have financial and organizational capacity, legal authority, satisfactory previous performance, skill, judgment and integrity, and that is found to be competent, reliable and experienced, as determined by the Central Procurement Office.
Responsive Bidder or Responsive Respondent	A Bidder or Respondent meeting the specifications or requirements prescribed in the Proposal Document or solicitation, as determined by the Central Procurement Office.
Request for Qualifications or RFQ	A type of Proposal Document that is used for procurements where factors in addition to cost are considered and weighted in awarding the contract.
Return Log	Any monies received by the TDA that are incorrect or not required should be logged onto a return log before being returned to the sender, noting the date they were received, who sent them, what type of payment they were, the date returned and the check number.
Revocation	Cancellation or withdrawal of a license permit, power, privilege or

TERM	DEFINITION
	act.
Routine Inspection	Agents usually try to conduct at least one routine inspection during a license year. Routine inspections are usually unexpected by the licensee. Generally the agent verifies that the establishment continues to meet their legal requirements, and that all licenses are properly posted. If the TDA receives a complaint on an establishment that needs investigation, an agent may conduct additional routine inspections at that establishment.
Rules & Regulations	The Tennessee Department of Agriculture has the authority to promulgate rules and regulations pertaining to license issued by TDA. These rules can be found on the TDA website at http://www.tn.gov/sos/rules/0080/0080.htm
Schedule of Events	The list of critical dates and actions included in the introductory materials.
Service Organization Control	**SOC 2 Type 2** This report and audit is completely different from the previous SOC 2 measures controls specifically related to IT and data center service providers. The five controls are security, availability, processing integrity (ensuring system accuracy, completion and authorization), confidentiality and privacy. Type 2 – Includes everything in Type 1, with the addition of verification of an auditor's opinion on the operating effectiveness of the controls.
	SOC 3 This report includes the auditor's opinion of SOC 2 components with an additional seal of approval to be used on websites and other documents. The report is less detailed and technical than a SOC 2 report.
Software Product	The software, including configurations and customizations, delivered to the State in accordance with the resulting Contract.
Software Product Verification	The pre-defined period during which the State monitors and verifies that system functions and system performance continue to meet Acceptance Criteria in the production environment.
Solicitation Coordinator	State of Tennessee representative for whom all communications relating to this solicitation shall be directed to.
Standard Manufacturer or Manufacturer's Warranty	An agreement which generally warrants against defects in workmanship or materials for a specified period of time after item purchase or shipment. The warranty shall be included in any sales agreement between the Contractor and the State for the purchase of goods and services specified in this RFQ. The length and terms of the warranty shall be specified and detailed before purchase.
State	State of Tennessee.
Status	The state of a TDA record [license/permit/education] at a particular time to be defined by business rules.
Subcontractor	Any individual or other legal entity, (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) that has entered into a contract, express or implied, for the performance of a portion of a Contract with a Contractor.
System Acceptance	The period in the project management lifecycle at which every aspect of the application phase being developed, along with any supporting data conversion routines and system utilities, is thoroughly validated ty by the TDA prior to proceeding with the System Implementation.

TERM	DEFINITION
System Implementation	The period in the project management lifecycle where the system is moved from a test environment to the live production environment and the system starts to be used for real business transactions.
System Requirement	A defined business function that is a required component of TDA system, specified in the RFQ and Appendix 6 Functional and Technical Requirements, as well as any detailed requirements established during the Business Process Reengineering and System Design phase of this project.
Surrender	When a licensed establishment closes, or no longer wishes to keep their license, they must surrender their license to the TDA. This means they should bring or mail in the actual license to the local TDA office along with a letter stating that they wish to surrender their license. When the TDA receives this, we will void your license.
Suspension	The temporary withdrawal of a license permit or privilege.
TDA	Tennessee Department of Agriculture
T.C.A. (Tennessee Code Annotated)	The Tennessee statutory law. (http://www.lexisnexis.com/hottopics/tncode/)
Transaction	Any activity carried out, performed, managed or conducted by a user of the system.
Transaction Log	A log that contains the history of transactions executed by the system and the user or operator associated with each transaction.
Transfer of Location	TDA licenses can request to transfer their location from one place to another. Appropriate documentation has to be submitted and approved prior to the move.
Unique Identifier	A string of characters that uniquely identifies a wide variety of entity/licensing items guaranteeing uniqueness with the entire system.
User	Anyone who employs the services provided by the system. The user can be an individual visitor to the TDA website, an applicant or licensee, a licensing agency staff member, or recipient of specific content from the system. See also Authorized User.
User Acceptance	Approval by the State that system functions and performance have met Acceptance Criteria after testing in a non-production version of the system.
Validity dates	The date range in which a license/permit/education is valid.
Violation	An incident where a licensee or other entity has broken a law or procedure in connection with their license/permit/education that TDA has been made aware of.
Weekly Report	Each week the TDA office issues a report showing all new licenses issued in the state, all voided licenses in the state, and all changes with licenses in the state for the prior week.
Weights & Measures	This program area monitors all commercial weighing and measuring devices in Tennessee. The devices inspected and tested include liquid fuel dispensers, bulk meters, LPG meters, and scales (small, medium, and large capacity). Inspections include net weight and price scanner verifications. The metrology laboratory calibrates volume and mass standards submitted to the laboratory; invoices are generated for the laboratory services provided.
Work Breakdown Structure (WBS)	A graphical representation of the hierarchy of project deliverables and their associated tasks. As opposed to a project Schedule that is calendar-based, a WBS is a deliverable-based, and written in business terms.
Workflow	Sequence of tasks. A workflow describes the order of a set of tasks

TERM	DEFINITION
	performed to complete a given procedure within an organization
Workflow Process	A series of steps through which work is routed.
Weekly Report	Each week the TDA office issues a report showing all new licenses issued in the state, all voided licenses in the state, and all changes with licenses in the state for the prior week.
Workflow System	A system which manages and defines a series of tasks within an organization to produce a final outcome(s)

	T.C.A.	Number
Weights & Measures		
Weighmaster License	47-26-1001	1,869
Certified Public Weigher Lic.	47-26-801	1,085
Serviceman Registration	47-26-1110	986
Pumps	47-26-909	
regular flow 1 - 6 pumps		759
regular flow 7 - 18 pumps		1,339
regular flow 19 - 36 pumps		1,860
regular flow 37- 54 pumps		454
regular flow 55 - 78 pumps		73
79 or more		9
High flow 1 - 6 pumps		234
6 or more		47
Scales (small)	47-26-909	
establishments with 1 - 5		3,370
establishments with 6 - 20		527
establishments with more than 20		200
Scales (large)	47-26-909	
1 to 2 large scales		935
3 or more larges scales		531
LPG/Bulk Meter	47-26-909	2,462
Bulk Mass Flow Meters	47-26-909	10
Retail CNG/LNG	47-26-909	10
Food & Dairy		
Meat & Poultry Inspection	53-7-219	
Custom Slaughter License	53-7-220	319
Vending Machine License	53-12-104(b)	
Egg License	53-2-109	56
Retail Food Store License	53-8-214	9,130
Food Manufacturers	53-1-208(3)(A)	1,304
High Risk		121
Medium Risk		418
Low Risk		687
Food Warehouses	53-1-208(3)(B)	512
High Risk		3
Medium Risk		133
Low Risk		373
Certificate of Free Sale	53-1-208(4)	797
Frozen Dessert Mfg. License	53-3-106(a)(1)	4
Distributor's Frozen Dessert Lic.	53-3-106(a)(4)	17
Distributor's Dairy Product Lic.	53-3-106(a)(4)	28
Dairy/Trade Products Mfg. Lic.	53-3-106(a)(2)	23
Dairy/Trade Products Registration	53-3-107(a)(1)	1,447
Milk Tester's License	53-3-105(b)	55

Milk Sampler's License	53-3-105(a)	196
AG Inputs		
Vendor to Wholesale Seed Lic.	43-10-118(a)(1)	105
Retail Agriculture Seed Lic.	43-10-118(a)(2)	2,833
Wholesale Agriculture Seed Lic.	43-10-118(a)(3)	185
Seedsman License		387
Seed Unit Fee >3000		3,961,714
Feed Tonnage (GF)	44-6-109, 44-6-104	
Feed Facility License	44-6-104(b)	1,388
Feed Tonnage Fee > 500 tons		6,548
Fertilizer Brand Registration	43-11-104	6,598
Fertilizer License (+tonnage fee + brand fee)		356
Tonnage Fee >1000 tons		576
Brand Fee >10 brands		904
Ag Liming Materials (license + tonnage fee)	43-11-405	57
Tonnage Fee >1000 tons		576
Plant Certification		
Nematode Sample Analysis	43-1-703(f)(7)	14
Plant Certificates - Nursery	43-1-703(f)(8)	653
Plant Certificates - Greenhouse	43-1-703(f)(8)	293
Plant Certificates - Plant Dealer	43-1-703(f)(8)	2,293
Phytosantitary Certificates	43-1-703(f)(15)	1,884
Pesticides		
Pesticide Dealer License	43-1-703(f)(11)	325
Pest. Applicator Certification Fee	43-1-703(f)(4)	5,070
Pesticide Product Registration	43-1-703(f)(13)	13,163
Special Local Need	43-1-703(f)(18)	2
Aerial Applicator	43-1-703(f)(1)	91
Aerial Decal	43-1-703(f)(2)	81
Pest Control Operator Fee	43-1-703(f)(9)	1,379
Pest Control Exam	43-1-703(f)(6)	365
Pesticide Private Applicator	43-1-703(f)(16)	688
Animal		
Certificate of Brand Registration	47-7-202 & 204	80
Livestock Dealer License	44-10-203	111
Livestock Market License	44-11-104	17
Baby Chick Law	44-16-202	139

Section	Report	Report ID
Agricultural Inputs		
	Ad Hoc Report	
	Anhydrous Ammonia Renewal status	
	Commercial Feed Samples by Dealer	
	Commercial Feed Samples by Manufacturer	
	Commercial Fertilizer Samples by Dealer	
	Commercial Fertilizer Samples by Manufacturer	
	Commercial Lime Samples by Dealer	
	Commercial Lime Samples by Manufacturer	
	Commercial Seed Samples by Dealer	
	Commercial Seed Samples by Manufacturer	
	Feed Licenses	
	Feed Tonnage Detail - date firm specified	
	Feed Tonnage Non-reporters	
	Feed Tonnage Summary - date firm specified	
	Feed Tonnage Top 50 Producers	
	Feed Tonnage Top Producers - date type	
	Feed Not Reporting	
	Fertilizer Data – Info retrieved from TFTRS	
	Inspector Performance Report	
	Lime facility renewal - tonnage status	
	Lime tonnage summary by county	
	Lime tonnage summary by region	
	Recent Samples	
	Recent Violations Report (Adjustable Range)	
	Seed List	
	Seed Reporting companies and licenses	
	State Report	
	Upcoming Inspections	
Civil Penalties		
	Civil Penalties: Issued for Previous Week	
	Civil Penalties: Pending	
	Civil Penalties: Delinquent	
	Civil Penalties: Paid	
	Civil Penalties: Delinquent Critical Item Letters	
Dairy		
	Broken Seal Tracking	
	Dairy Inspection Summary Need for plants also	
	Dairy Permit Summary	
	Dairy/Trade Product Registration	
	Distributors License	
	Double Debit and Triple Debit Report (Need for plants also)	
	Equipment tests for plants	
	Farm History Report	
	Farm Inspection Detail Report	
	Farm Inspection Summary Report	
	Farm Listing Report	

Section	Report	Report ID
	Farm Mailing Labels	
	Farms and Plants Requiring Water/Glycol/Sweetwater Sample	
	Frequencies of Inspections Done	
	Industry Emergency Sealer Personnel Tracking	
	List Number of Active Farms by BTU	
	Milk Sample Results Upload Rejection Report	
	Milk Sample Summary	
	Notification of Failure to Receive Surety Bond	
	Producer Reinstatement Status Report	
	Random Survey Report	
	Sample Deficiency Report Need for plants also	
	Sampler / Hauler tracking for recertification/permitting	
	Sampler Mailing Labels	
	Sampling Surveillance Officer Tracking (SSO) / Delegate Sampling Surveillance Officer (DSSO)	
	Somatic Cell Info – Qualify % Information	
	Surety Bond Tracking	
	TDA Grade A Dairy Farm & Plant Inspection Report (Past 24 Months)	
	Truck Permit/Inspection Tracking	
	Warning Status Report Need for plants also	
	Warning/Penalty Count/Suspension/Penalty List	
Dairy - Other Program Areas		
	Eggs - Annual Permit	
	Eggs - Fee Reconciliation	
	Eggs - Inspection Report	
	Vending - Annual Permit	
	Vending - Fee Reconciliation	
	Vending - Inspection Report	
	Meats (Custom Slaughter or Meat Processors) - Annual Permit	
	Meats (Custom Slaughter or Meat Processors) - Fee Reconciliation	
	Meats (Custom Slaughter or Meat Processors) - Inspection Report	
Food Safety		
	Food Establishments By County Report	
	Food Establishment Uninspected Report	
	Food Establishment Profile Detail Listing	
	Retail Food Establishment to Sample	
	Civil Fines Summary Report	
	Previous Inspection Data	
	Weekly Food Reports: Emergency Contact List	
	Weekly Food Reports: Profile List	
	Weekly Food Reports: New Profile Listing	
	Weekly Food Reports: Renewal Report	
	Weekly Food Reports: Device Only Establishments	
	Areas Closed	
	Seizures and Condemnations	
Food Safety - Tobacco		
	Tobacco: Establishment Compliance	

Section	Report	Report ID
	Tobacco: Establishment History	
	Tobacco: Complete Report	
	Tobacco: Incomplete Report	
	Tobacco: Sign Posted Recap	
	Tobacco: Enforcement Summary (By Year)	
	Tobacco: Enforcement Summary (By Month/Year)	
	Tobacco: Compliance	
	Tobacco: Enforcement Fines	
	Tobacco: Generated Sign Fines	
	Tobacco: Yearly Report	
General Financial		
	Financial: CD Report	
	Financial: Revenue	
	Financial: Account Detail Report	
	Financial: Register Report	
	Financial: Refund Report	
Pesticide - Certification Testing		
	History of activity of taking license and certification exams	
	Refunds requesting for testing	
	Report by location, category of license and certification exam scheduled and taken	
	Report by name, address, city, state, zip, phone and email address	
	Report by pass, fail, score and no show	
	Report fees paid for certification exams requested and by category of exam	
	Report number missing the questions administered (item analysis)	
	Report number of company employees taking test for the 1st time vs repeat request	
	Report number of confirmations sent and returned	
	Report number of days blocked out for test not to be administered	
	Report number of seats filled and available for testing	
	Report number requesting special testing sessions (written, category and by date)	
	Report of questions missed with the correct and incorrect answer	
Pesticide – Chartered Pest Control Companies		
	History of Activity for all companies	
	Report by name, address, city, state, zip, county, phone number and email address	
	Report Notice of Violation and Enforcement Actions issued by rule and regulation	
	Report number of applicators connected to a charter including licenses and certifications	
	Report number of refunds requested and dollar amount	
	Report of all pest control companies that have paid renewal fees and civil penalties, those not paid and delinquent	
	Report of companies inspected and needing to be inspected	
	Report of companies out of business and brought out	
	Report of current and expired bond and insurance	
Pesticides – Complaints		
	History of Activity	
	Report number of complaints assigned by inspector and supervisor and who	

Section	Report	Report ID
	initiated the complaint	
	Report number of complaints by type, including illegal operators	
	Report number of complaints received, by name, address, city, state, zip, county, phone and email address	
	Report number of days to close complaint	
Pesticides – Enforcement		
	EPA Reports and Performance Measures	
	History of Activity	
	Report by applicator, company, ID number, name, address, city, state, zip, county phone, and email address	
	Report civil penalties paid, owed and delinquent	
	Report number of administrative hearings conducted, date, reason, and outcome	
	Report number of days from start to close inspections	
	Report number of informal discussions held, date, results, date case closed, rule and Regulation	
	Report number of Notice of Violation and Enforcement Actions issued by rule and regulation and by inspection type	
	Report number of routine, follow-up, complaint, inspection type and total number of Inspections	
	Report number of samples collected, analyzed, sample type and results	
Pesticides – Pesticide Applicators (Commercial, Private, Licensed, including Limited Herbicide Applicator (LHA))		
	EPA reports and CPARD (Certification Plan and Reporting Database)	
	History of activity for all applicators	
	Insurance for Aerial	
	Renewals for all licensed applicators	
	Report by name, address, city, state, zip, county phone and email address	
	Report categories of certifications and license issued, current and expired	
	Report decals assigned to Aircraft & Aircraft number	
	Report fees and civil penalties paid, owed and delinquent	
	Report Notice of Violation and Enforcement Actions Issued by rule and regulation	
	Report number of certification cards issued	
	Report number of recertification letters sent to private applicators	
	Report number of refunds requested and dollar amount	
	Report of applicators deceased and removed from chartered companies	
	Report of applicators with accrued CEU's and needing CEU's by category of certification	
Pesticides – Products and Manufacturers		
	Fees and civil penalties paid, owed and delinquent	
	History of activity	
	Renewals for all products expiring on a yearly basis	
	Report by ID number assigned, type, use, EPA Registration number, discontinued, RUP (Restricted Use Pesticide) current and expired	
	Report by manufacturer name, address, city, state, zip, phone, email and state contact	
	Report Notice of Violation and Enforcement Actions issued by rule and regulation	
	Report number of refunds requested and dollar amount	
Pesticides – Restricted Use Pesticide Dealers		

Section	Report	Report ID
	Category 12 Pesticide Dealer current and expired listed by name and ID number assigned	
	EPA reports	
	History of activity for all dealers	
	Report by name, address, city, state, zip, county, phone and email address	
	Report fees and civil penalties paid, owed and delinquent	
	Report inspected and needing to be inspected	
	Report Notice of Violation and Enforcement Actions issued by rule and regulation	
	Report number of refunds requested and dollar amount	
	Report of dealers out of business	
Pesticides – WPS – Worker Protection Standard		
	EPA reports and CPARD (Certification Plan and Reporting Database)	
	History of Activity	
	Report category of certification trainer holds and expiration date	
	Report persons conducting training by name, address, city, state, zip, county, phone number and email address	
	Report worker and handlers current and expired	
Plant Certification		
	Certified Sod Certificate	
	Educational Organization Certificate	
	Florist Dealer Certificate	
	Greenhouse Certificate	
	Hemp License Certificate	
	Hobbyist Greenhouse Certificate	
	Hobbyist Nursery Certificate	
	Landscaper Certificate	
	Limited Plant Dealer Certificate	
	Native Wild Plant Dealer Certificate	
	Nursery Certificate	
	Plant Dealer Certificate	
	Sweet Potato Seed Dealer Certificate	
	Sweet Potato Slip Certificate	
Point to Point		
	Inspector Task Profile Report for Section - Animal Health	
	Program Activity Summary for Section - Animal Health	
	Program Summary for Section - Animal Health	
	Point to Point by Inspector - Ag Inputs	
	Point to Point (PTP) Reporting - Ag Inputs	
	Point to Point - Day (Dups filtered out) - Ag Inputs	
Revenues		
	Revenue: Unpaid Fee Summary	
	Revenue: Scantron Rejection Report	
System Wide Reports		
	Quarterly: Performance Report	
	Quarterly: Frequency of Violations	
	Quarterly: Facility Statistics Report	
	Quarterly: Scoring Level and Workload	

Section	Report	Report ID
Tobacco Compliance		
	Mental Health Report	
	Tobacco Report	
Weight and Measures / Petroleum Quality		
	Annual Report on the Quality of Kerosene and Motor Fuel in Tennessee – (by FY)	
	Bulk Meter Inspection Summary	
	Certificate of Analysis Report – By Product Types and/or Grades	
	Checkweighing Report	
	Checkweighing Report - By County, By Inspector, By Type	
	Checkweighing/Price Verification Detail	
	Consumer Complaint Report (Various parameters)	RedBarn
	Device Inspection Summary	
	Establishments With Devices Detail	
	Establishments With Devices Summary	
	Fines (Various parameters)	RedBarn
	LPG Meter Inspection Summary	
	Meter/Inspection Summary Report - (Meter Type)	
	Notice of Violation and Issuance of Enforcement Action	
	Product Violation Analysis Report	
	Price Verification Report	
	Price Verification Report - By County, By Inspector	
	Pump Inspection Summary	
	Report of Petroleum Storage Tanks Testes	
	Report of Weighing and Measuring Devices Tested (BNK-NOZ)	
	Report of Weighing and Measuring Devices Tested (Scale)	
	Report of Weighing and Measuring Devices Tested (Serial)	
	Report of Weighing Devices Tested	AG-0226
	Service Agencies by Type	
	Statistical Reports	
	Stop Sale (Various parameters)	RedBarn
	Summary of Establishments with Devices	
	Uninspected Establishments	
	Uninspected Establishments Devices	
	Violation Analysis Report	
	Weights and Measures Statistical Report	
	Weights and Measures Numbers Report	
	Weights and Measures Scantron Import Report	
	Violation Analysis Report	

Section	Form	Form ID
Agricultural Inputs		
	Ag Establishment Inspection Report	AG-0605
	Certification of Grain Payments Within 30 Days of Delivery	
	Chain of Custody Record for Samples	AG-0583
	Extension Request	
	Generic Field Stop Sale & Seizure Notice	AG-0483
	Indemnity Fund Monthly Report	
	Nonresident Exemption	AG-0487
	Not a Purchaser of Grain from Producers	
	Proof of Claim	
	Refund of Grain Indemnity Fund Assessment	AG-0486
	Sample Report	AG-0488
	Tennessee Commodity Producer Indemnity Fund Monthly Report	
	Tennessee Grain Indemnity Fund - Proof of Claim	
Animal Health		
	Application for Livestock Brand Registration	AG-0052
	Application for Tennessee Baby Chick Sale License	AG-0061
	Application for Tennessee Livestock Dealer License	AG-0064
	Livestock Market License Application	AG-0675
	Slaughter Swine Form	AG-0690
Apiary		
	Apiary Inspection Health Certificate	
	Apiary Inspection Request	
	Apiary Pest and Disease Specimen Form	
	Apiary Registration Form	
	Apiary Section Complaint Form	
	Application to Establish an Experimental Apiary in TN	
	Application to Move Honeybees or Used Equipment into TN	
	Customer Complaint Form	
	Honeybee Best Management Practices Agreement	
	Honeybee Best Management Practices Policy	
	Reporting Movement of Honeybee Colonies for Pollination within TN	
	Request for Apiary Information	
	Request to be Placed on List to Sell Local Honey and Other Products	
	Request to be Placed on Pollinator List for Growers	
	Request to be Placed on Structural Honeybee Removal List	
	Request to be Placed on Swarm Removal Services List	
	Request to be Removed From Any or All Above Lists	
Dairy Inspections - Applications		
	Application for Dairy Plant and/or Trade Products Plant License	
	Application for Distributors License	
	Application for Frozen Dessert Manufacture's License	D-5
	Application for Grade 'A' Milk Permit	
	Application for License Processing or Slaughtering of Meat and Poultry	
	Application for Registration of Dairy and-or Trade Products	AG-0354
	Application for Reinstatement of Permit	
	Application for Reinstatement of Sale of Product	

Section	Form	Form ID
	Application for Temporary Permit Status and Authorization for Civil Penalty Deduction	
	Application for Tennessee Egg License	
	Application for Tester's License	D-3
	Application for Vending Machine and Commissaries License	
	Sampler's/Weighmaster License Application	
Dairy - Inspection Reports (FDA) – Convert to TN Form		
	Bulk Milk Hauler-Sampler Evaluation Report	FDA 2399a
	Dairy Farm Inspection Report	FDA 2359a
	Manufacturing Plant Inspection Report – Single Service	FDA 2359c
	Milk Plant Equipment Test Report	FDA 2359b
	Milk Plant Inspection Report	FDA 2359
	Milk Sample Collector Evaluation Report - Dairy Plant Sampling - Raw and Pasteurized Milk	FDA 2399b
	Milk Tank Truck Inspection Report	
	Permission for Publication	FDA 2359o
	Report of Certification	FDA 2359d
Feed, Seed and Fertilizer		
	Annual Agricultural Liming Material Tonnage Report	
	Application for a Commercial Feed Facility License	
	Application for Seed License	AG-0308
	Application to Register Fertilizers	AG-0336
	Feed Tonnage Report	
	Grain Dealer License (Class 1 or 2)	AG-0627
	Incidental Grain Dealer	AG-0625
	License Application for Manufacturers of Commercial Lime	
	Public Grain Warehouse License	AG-0626
	Quarterly Fertilizer Tonnage Report	AG-0294
	Quarterly Report of Agricultural and Vegetable Seed Sold	AG-0687
Food and Dairy - Domestic Kitchen Permit		
	Domestic Kitchen Questionnaire	
	Sample Application Form	
Food and Dairy - Manufacturing Warehouse Permit		
	Plan Review Questionnaire	
	Sample Application Form	
Food and Dairy - Manufacturing Within Existing Establishment		
	Plan Review Questionnaire	
	Sample Application Form	
Food and Dairy - Other Permits		
	Sample Commercial Slaughter Application	
	Sample Egg License Application	
	Sample Vending Machine Application	
Food and Dairy - Retail Food Permit		
	Basic Requirements	
	Retail Request	
	Sample Application Form	
Food and Dairy - Retail Mobile Food Permit		

Section	Form	Form ID
	Farm Based Retail Meat Sales	
	Retail Plan Questionnaire	
	Sample Application Form	
Food and Dairy - Retail Mobile Seafood Permit		
	Retail Plan Questionnaire	
	Sample Application Form	
	Seafood Guidance	
Other Forms		
	Application - Registration of Farm Names	
Pesticides		
	Aerial Applicator Verification Form	AG-0137
	Additional Comments and Violations	AG-0609
	Application for Aerial Applicator License	
	Application for Duplicate or Replacement Certification Card	
	Application for Reciprocity in the State of Tennessee	
	Application for Restricted Use Pesticide Dealer License	
	Application for the Registration of Pesticides in Tennessee	
	Application to Take Certification Exam	
	Application to Take Commercial Pest Control License Exam	
	Apprentice Termite Technician School Registration Form - June	
	Apprentice Termite Technician School Registration Form - March	
	Apprentice Termite Technician School Registration Form - September	
	Certificate of Surety Bond for all other categories	AG-0105
	Certificate of Surety Bond for WDO, General Pest and Rodent, Bird, and Fumigation Structural	AG-0105
	Chain of Custody Report for Samples	AG-0583
	How to Complete the Product Registration Application	
	How to Obtain an Aerial Applicator License and Aircraft Decal	
	Marketplace Dealer Inspection Report	AG-0587
	Notice of Inspection	AG-0340
	Pest Control Applicator License and Charter (companies a-k)	
	Pest Control Applicator License and Charter (companies l-z)	
	Pesticide Application Inspection Report	AG-0586
	Pesticide Containment Checklist Report	
	Pesticide Investigation Request Form	AG-0568
	Pesticide Inspection Request Form	
	Pesticide Use Review Report	AG-0586
	Producer Establishment Inspection Report	
	Reciprocity Form for the State of Tennessee	
	Refillable Pesticide Container Checklist	
	Roster for Commercial Pesticide Applicator Recertification Point System in Tennessee	E&PP Info #81
	Sample Collection Report	
	South Carolina Non-refillable Pesticide Container Inspection	
	Statement	AG-0645
	Tennessee Pesticide Recertification - Application for Points	E&PP Info #82
	Termicide Calculation Sheet	

Section	Form	Form ID
	UT Pesticide Certification & Licensing Study Material Order Form	
	WPS Employee Interview	
	Worker Protection Use Inspection Report #1	AG-0554
	Worker Protection Use Inspection Report #2	AG-0556
Plant Certification		
	Application - Florist Certificate	
	Application - Greenhouse Certificate	
	Application - Hobbyist Greenhouse Certificate	
	Application - Hobbyist Nursery Certificate	
	Application - Landscaper Certificate	
	Application - Native Wild Plant	
	Application - Nursery Certificate	
	Application - Plant Dealer Certificate	
	Christmas Tree Inspection Report	
	Compliance Agreement – Cornus spp.	
	Compliance Agreement – Boxwood Blight	
	Compliance Agreement – Firewood	
	Compliance Agreement – Imported Fire Ant	
	Compliance Agreement – Japanese Beetle Harmonization	
	Compliance Agreement for Movement of Bare Root Stock into Oregon	
	Consumer Complaint Form	
	Emergency Action Notification	
	European Corn Borer Shipping Notification Permit	
	General Inspection Report	
	Greenhouse Inspection Report	AG-0100
	Hobbyist Greenhouse Certificate	AG-0592
	Hemp Movement Permit	
	Imported Fire Ant Monthly Report	
	Insect and Plant Disease Specimen Form - 1 eMail address	
	Insect and Plant Disease Specimen Form - 2 eMail addresses	
	Inspection Report	
	Native Wild Plant Inspection Report	AG-0099
	Nursery Inspection Report	AG-0100
	Permit for Movement	AG-338
	Plant Dealer Inspection Report	
	Shipping Quarantined Articles from European Corn Borer Infested Areas to Free Areas of Texas - Packer Shipper Agreement	
Time Management		
	Animal Health Version 5.1 111414	
Weights and Measures / Petroleum Quality		AG-0406
	Bulk Meter Test Report	AG-0220
	Certified Public Weigher License Application	
	Check Weighing & Price Verification Summary	
	Consumer Complaint	
	Grain Moisture Meter Report	
	Hopper Scale Test Report	P&SP-4500
	Official Notice of Equipment Rejection and/or Violation	AG-0225

Section	Form	Form ID
	Livestock Scale Test Report	P&SP-4200
	LPG Meter Examination	AG-0229
	Monorail Scale Test Report	P&SP-4300
	Petroleum Sample Collection Form	AG-0479
	Permit - Certified Public Weigher	
	Permit - Public Weight Master	
	Permit - Service Agency License	
	Permit - Service Person	
	Regulatory Services - Daily Time Log	AG-0581
	Random Pack Report	AG-0564
	Report of LPG Meter Examination	AG-0229
	Report of Price Verification System Inspection	AG-0558
	Report of Weighing Devices Tested	AG-0226
	Request for Inspection	
	Serviceperson Agency Application	AG-0178
	Serviceperson Application	
	Standard Pack Report	AG-0565
	Stop Sale Order and/or Seizure/Condemnation	AG-0483
	Terminal Meter Test Report	AG-0458
	Vehicle Scale Test Report	P&SP-4400
	W & M Device Fee Invoice	
	Weekly Summary and Itinerary	AG-0454
	Weighmaster License Application	AG-0193

Contractor Requirements

The Contractor will provide the Deliverables and meet the requirements specified in the Contract and its referenced attachments. The Contractor shall perform all of the activities and tasks required to achieve the objectives, functions, outputs, and performance criteria stated in the Contract. All services provided by the selected Contractor shall be appropriate and acceptable to the TDA project team and be consistent with State and Federal laws and regulations. The Contractor shall provide all of the staff necessary to perform the required services.

During the life of the project, the State will review Deliverables and evaluate them for completeness, clarity, adherence to generally recognized standards, and compliance with the contract. A Deliverable phase or milestone will not be considered complete until written approval has been given by the State. The process by which all Deliverables will be reviewed and accepted is outlined in Deliverable Acceptance.

The system will run in computing facilities maintained and operated by the Contractor. The State requires that the Contractor follow a systematic approach to the design, development, and implementation of the System to ensure that a comprehensive and expandable system is implemented. The State of Tennessee's Information Technology Methodology is Tennessee Business Solutions Methodology (TBSM). TBSM is based on the principles set forth by the Project Management Institute (PMI) and on industry best practices that are adapted to meet the state's needs. The contractor will be required to utilize these templates or templates comparable to the TBSM. The Contractor should address all the Deliverables for the life-cycle phases in their project plan but can organize and plan for the accomplishment of the work based on their experience with projects of similar scale and scope. The complete detailed requirements, which identify the required functionality of the System, are provided in Appendix 2 – *Functional and Technical Requirements*.

The contractor shall define the overall Project Management approach for the project and should describe, in general terms, the roles and authorities of project team members from both the State staff and the Contract staff. The Project Management Approach should be based on the Contractors best practices and experience, and should be fully described in the section of the Project Management Plan. The Contractor confirms their commitment to meet all requirements defined in this Appendix regardless of the approach proposed.

Each of the following subsections provides a narrative on the requirements, followed by a table defining the tasks and Deliverables to be fulfilled by the Contractor.

The Contractor shall provide project Deliverables for the system in the form and format agreed to by the State.

Project Initiation

The Project Initiation activity includes project planning for work performed for the TDA project contract. The complexity of the proposed System will require significant access and involvement of licensing Subject Matter Experts (SMEs).

During this activity, the project schedule will be developed, refined and confirmed, and risk assessment activities advance to the mitigation stage. The initial Project Schedule and Project Management Plans - are further developed, enhanced, and refined until they form a definitive plan for the rest of the project. The Contractor and the State will develop their project performance measures and collect the data to establish baseline performance. Contractor Deliverable or process requirements (CR) for the Project Initiation activities are described in Table 1.

Table 1, Project Initiation Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 1.	The Contractor shall identify the Project Management Approach which includes specific needs for information, materials, and decisions for TDA prior to the start of the Project Initiation phase of work proposed by the Contractor and request such information in writing. [See *Pro Forma* Contract Section A.3]	Project Management Approach
CR 2.	The Contractor shall refine and deliver its proposed project plans consistent with the resulting contract, including: • Project Scope Management Plan; • Milestone List; • Project Schedule Baseline; • Work Breakdown Structure (WBS); • Activity List; • Change Control Process; • Human Resource Plan; • Quality Management Plan; • Risk Management Plan; • Acceptance Management Plan; • Change Management Plan; • Issue Management and Escalation Plan; • Communication Management Plan; • Cost Management Plan; • Development, Implementation, and Transition Plans (including migration plans); • Requirements Development Plan; • Schedule Management Plan; • Performance Management Plan; • Training Plan; and • Fit/Gap Analysis	Project Plan
CR 3.	The Contractor shall refine the project schedule, including the project timeline, all major milestones, work breakdown structure, and a list of technical assumptions.	Project Schedule
CR 4.	The Contractor shall refine the project schedule, including defining the sequencing of project activities, the durations of the project activities, and any dependencies among the project activities for both the Contractor and State activities to create an agreed and approved project schedule baseline.	Master Project Schedule
CR 5.	The Contractor shall deliver the project schedule in MS Project format.	Project Schedule
CR 6.	The Contractor shall refine and deliver a project staffing plan that identifies individual resources (both State and Contractor resources) assigned to each of the project activities.	Staffing Plan
CR 7.	The Contractor should provide a Fit/Gap analysis. The analysis shall document, at a detailed level the extent to which the Proposer's software can meet the TDA required functions.	Requirements Verification and Fit/Gap
CR 8.	The Contractor shall describe the strategy that will be used to acquire human resources with the appropriate skills to staff the project.	Staffing Plan
CR 9.	The Contractor shall maintain job responsibility statements on file for all project personnel, including subcontractors and shall provide a copy to the State.	Human Resource Plan
CR 10.	The Contractor shall maintain and provide to the State an up-to-date organization chart and contact list providing name, title, phone, pager/cell phone, and email information for all Contractor personnel assigned to the project whenever Contractor personnel assignments change.	Human Resource Plan

Contractor Requirements		
	Task	**Deliverable or Process**
CR 11.	The Contractor shall refine and deliver a quality management plan that documents the quality standards and service level requirements of the project.	Quality Management Plan
CR 12.	The Contractor shall refine and deliver a quality management plan that documents all quality assurance activities to be implemented during the lifecycle of the project.	Quality Management Plan
CR 13.	The Contractor shall refine and deliver a risk management plan that shall include specific activities the Contractor will regularly perform to identify, qualify, quantify, prioritize, and manage risks.	Risk Management Plan
CR 14.	The Contractor shall refine and deliver a risk management plan that describes the actions to be taken to avoid, mitigate, or accept each risk impact.	Risk Management Plan
CR 15.	The Contractor shall refine and deliver a risk management plan that defines the frequency of risk management activities and status reporting.	Risk Management Plan
CR 16.	The Contractor shall work with the State to refine and deliver an acceptance management plan for the review and approval by the State of all project Deliverables including document-based Deliverables and software-based Deliverables.	Acceptance Management Plan
CR 17.	The Contractor shall refine and deliver a change management plan that describes the process for making any adjustment to any aspect of the project plan or to any already approved Deliverable(s). This includes anything formally documented in the project plan or any Deliverable produced during the course of the project.	Change Management Plan
CR 18.	The Contractor shall work with the State to refine and deliver a change management plan for the project that includes: • Identification of who is authorized to request a change; • Identification of who is responsible for analyzing the request's impact on the Project Cost, Scope, Schedule, and Quality; • Identification of who has authority to approve the request; • The timeframe (number of business days) allowed for a change request to be approved or rejected; • The process to follow if no timely decision on approval or rejection of a change request is made; and • The percentage of the overall Project Budget that has been reserved for project changes.	Change Management Plan
CR 19.	The Contractor shall refine and deliver an issue management plan for the project that includes: • How issues will be captured and tracked; • How issues will be prioritized; • How issues will be assigned; and • How and when issues will be escalated for resolution.	Issue Management and Escalation Plan
CR 20.	The Contractor shall refine and deliver a communications plan that describes how communications will be managed on the project, including: • How project information will be collected and stored, and what procedures will be followed to disseminate the information; • The distribution structure, specifically detailing what, how, and when information will flow to stakeholders; and • The method by which information will be accessed if it is needed between regularly scheduled communications.	Communications Plan

Contractor Requirements		
	Task	**Deliverable or Process**
CR 21.	The Contractor shall refine and deliver the project implementation and transition plans for implementing or deploying the System and for transitioning the responsibility of system operation from the Contractor to the State. This plan includes all the necessary activities to perform and procedures to follow to ensure a smooth and satisfactory hand-off.	Development, Implementation and Transition Plans
CR 22.	The Contractor shall refine and deliver the development, implementation, and transition plans, including: • A description of what needs to be done to ensure the State will be ready to receive the System; • An early assessment of agency readiness to allow mitigation of significant risks exposed by the assessment; • A description of how and when the Contractor recommends that the State will test and accept the System and confirm and authorize its implementation; • The steps to be taken to ensure that users will be ready to use the System once it is transitioned; • Recommended adjustments to the strategy for implementing the System (for example, phased by Participating Agency, specific license type(s), license function or other); • The steps that should be taken to ensure that the appropriate individuals are ready to support the System once it has been implemented and is in use; • Identification of the point in implementation at which the State takes responsibility for production problems, "help" or trouble calls, and for resolving the problems; • Identification of user and technical documentation to be delivered as part of the transition; and • Knowledge transfer approach describing how the State staff members will administer, maintain and support TDA without Contractor intervention.	Development, Implementation and Transition Plans
CR 23.	The Contractor shall refine and deliver a data conversion/data migration plan including: • A description of what the State needs to do to prepare existing data for import into the software database; and • How and when the State will test the validity and integrity of imported data.	Development, Implementation and Transition Plans
CR 24.	The Contractor shall provide a performance management plan that will include a detailed description of the methodologies, tools, and procedures in which the Contractor will manage and measure performance. The plan must also provide a listing of the items that will be measured, frequency of measurement, and appropriate metrics.	Performance Management Plan

Project Management

The Contractor shall designate a Project Manager to whom all communications may be addressed and who has the authority to act for the Contractor in all aspects of the services to be performed pursuant to this contract. The Project Manager will be responsible for directing the work of the Contractor's staff. For a full description of how the State expects to govern and manage the project please refer to *Pro Forma* Contract A.3.

The Deliverable requirements for the project management activities are described in the table below:

Table 2, Project Management Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 25.	The Contractor shall update and implement the project quality management plan.	Quality Management Planning
CR 26.	The Contractor shall update and implement the risk management plan.	Risk Management Planning
CR 27.	The Contractor shall update and implement the project change control process.	Change Control Planning
CR 28.	The Contractor shall update and implement the project issue management and escalation process.	Issue Management Planning
CR 29.	The Contractor shall update and implement the project communication plan.	Communications Planning
CR 30.	The Contractor shall monitor the project for performance in accordance with baseline projections established within the contract deliverable dates. The Contractor Project Manager shall immediately advise the State Project Manager in writing, anytime it is determined the State Project team or the Contractors performance is jeopardizing the Project Work Plan, Project Scope, or the Project Budget. Any identified performance or delivery of critical path tasks/activities that could pose potential modification to the baseline work plan/schedule would be required to be presented to the Project Steering Committee and Change Control Board for review and approval.	All Phases/Project Schedule
CR 31.	The Contractor shall implement the project development, transition and implementation process.	Development, Transition and Implementation Management Planning
CR 32.	The Contractor shall attend all project meetings, including, but not limited to: • Kickoff Meeting – Within two weeks of final contract approval from the TDA, a kickoff meeting will be held at State offices to discuss start-up procedures; • Project Development Meetings – meetings related to project development and implementation as defined in the project communication plan and project schedule; • QA Meetings – quality assurance and review meetings as specified in the Contractor's Quality Assurance Plan; • Status Meetings – There shall be weekly project status meetings to review the progress and status of the tasks, problem areas, work to be accomplished, and other relevant items. Other ad hoc or periodic status meetings may be scheduled for specific communications needs; • Project Steering Committee Meetings – There shall be monthly Project Steering Committee meetings held at State offices to provide State staff and stakeholders with project status and accomplishments to date. The Contractor shall be responsible for preparing pre- and post-meeting documentation.	Communications Management Plan

Contractor Requirements		
	Task	**Deliverable or Process**
CR 33.	The Contractor shall provide status reports (periods to be determined by the State) to the State Project Team on the status of design and development metrics tasks, and milestones, including but not limited to: • Requirements status; • Design status; • Development status; • Test status; • Issue status; • Implementation status; and • Schedule status.	Communications Plan
CR 34.	Monthly Reporting Plan View - State requires a monthly status report for each project. The report is entered and updated in the State Project Portfolio Management tool, Plan view. Contractor will be responsible for providing required data elements for Plan view updates to this Project.	Communication Plan
CR 35.	Issue reports generated by the issue tracking system shall become part of Contractor's Status Reports.	Communications Plan
CR 36.	The Contractor shall provide the ability for initial issue creation and ongoing access/tracking of the issue tracking system to key State staff as designated by the State.	Issue Tracking System
CR 37.	The Contractor will develop a list of key performance measures and problem indicators jointly with State project management.	Performance Measures
CR 38.	The Contractor shall ensure that project Deliverables shall be subject to State review and approval prior to acceptance.	Acceptance Management Plan
CR 39.	The Contractor shall ensure that each project Deliverable is submitted to the State for review and acceptance with an approved deliverable specification sheet (to be developed jointly between the Contractor and the State after contract award).	Acceptance Management Plan
CR 40.	The Contractor shall ensure that each Deliverable shall address all components required by the contract including any areas identified subsequently through meetings and planning sessions, and the approved deliverable specification sheets.	Acceptance Management Plan
CR 41.	The Contractor shall certify in the cover letter for each Deliverable that the Contractor's internal deliverable review process was utilized.	Acceptance Management Plan
CR 42.	The Contractor shall ensure that for document-based Deliverables, the review and acceptance period reflects the time periods outlined in *Pro Forma* Contract A.10.a	Acceptance Management Plan
CR 43.	For Deliverables that contain hardware and/or software programs, the State's deliverable review process will incorporate acceptance testing as detailed in State approved Acceptance Test Plan.	Acceptance Management Plan
CR 44.	The Contractor shall ensure that, in the event the State agrees to accept, on an interim basis, a Deliverable with one or more sections left incomplete, the Deliverable shall include the date for completion, note the basis for the incomplete portions and the impact of any incomplete sections on project milestones.	Acceptance Management Plan
CR 45.	The Contractor shall identify in the project work plan the key documentation delivery milestones.	Project Schedule
CR 46.	The Contractor shall provide electronic copies of all documentation to the State in the format specified by the State, and supply hard copies as requested.	Development, Transition and Implementation Management Planning

Business Process Re-engineering

Business process re-engineering is required to develop the "To Be" in the TDA for the System. TDA have already invested considerable effort in documenting the current "As Is" business processes and will work with the Contractor to determine where improvements can be made.

Contractor Deliverable requirements for the business process re-engineering activities are described in the table below.

Table 3, Business Process Re-engineering Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 47.	The Contractor shall review existing "As Is" business process documentation, where it exists, and conduct a series of workshops with process stakeholders to confirm the "As Is" information and to ascertain changes that are required to complete the process documentation. Where "As Is" documentation does not exist, the Contractor shall conduct a series of workshops with process stakeholders to create the "As Is" business process documentation.	"As Is" Process Analysis
CR 48.	The Contractor shall review current business processes and develop an initial set of findings related to current processes. These findings will provide TDA with the rationale for the findings, the processes affected, the impact on the business function, and how improvement could positively affect the business function.	Review of Current Business Processes
CR 49.	The Contractor shall develop recommendations for process transformation based on the review of current processes. The Contractor shall document the areas for improvement identified and group the recommended business changes according to characteristics such as: changes to basic operating procedures; standardizing documentation; implementation of new technology; streamlining of current business processes; roles and responsibilities of organizational units; and changes to laws, policies, and regulations.	Recommendations for Process Transformation
CR 50.	The Contractor shall develop recommendations to address specific process improvement steps required by the business changes defined in the previous CR. The Contractor will provide short- and long-term process improvement recommendations based on this analysis. These recommendations will highlight specific procedural areas for improvement and demonstrate related improvement opportunities. For each recommendation, the Contractor shall identify: benefits to be gained; effect on process timeliness; estimated Return on Investment (ROI); impact on the organization; and re-defined process steps.	Recommendations for Process Transformation
CR 51.	The Contractor shall work with TDA to finalize and prioritize recommendations. Prioritization will be based on the potential benefits to be gained, timeframes in which to implement, ROI, process time efficiencies to be gained, and other environmental factors.	Recommendations for Process Transformation
CR 52.	The Contractor shall develop "To Be" process maps for each of the processes, depicting the new process with an analysis of the change in workflow.	"To Be" Process Maps
CR 53.	The Contractor shall develop an implementation plan that will serve as a roadmap for the TDA. This task will focus on the timeframe for implementation of changes to processes and procedures, and providing guidance on short- and long-term implementation depending on the nature of the recommendation.	BPI Implementation Plan

Organizational Change Management (OCM)

This OCM collaboration should also focus on reducing resistance and increasing speedy adoption and productivity during and after the implementation of the future state. This should include, at minimum, an end user Communication Plan, a Training Plan and a comprehensive Change Initiatives Plan. The expected outcome of the OCM Strategy is to reach ultimate productivity and business results as quickly as possible.

Table 4, Organizational Change Management

Contractor Requirements		
	Task	**Deliverable or Process**
CR 54.	The Contractor shall co-create, in conjunction with the State, an Organizational Change Management (OCM) Strategy. If the contractor does not already have knowledgeable OCM resources, the Contractors' Project Team will be working with an existing State OCM resource.	"Organizational Change Management Plan [assistance]

System Design

The purpose of System Design is to configure a technical solution that satisfies the functional requirements for the System. It is understood that a commercial software product has its own inherent design, so individual license/permit types will have to be retrofitted to that design, and/or customization of the software product may be undertaken to meet the State's requirements. As such, the Contractor, with TDA's assistance, will undertake a System Design effort that must occur for each license/permit type. This activity begins with a detailed review and analysis of the functional requirements to confirm a common understanding of how to evolve the requirements into the system design. The requirements are mapped to the enterprise architecture, and technical specifications are created for the implementation team, enabling them to configure and test the System. System Design is the time to initiate focused planning efforts for both the testing and data preparation activities. Test descriptions are to be developed, traced to requirements, and include the expected test results. Contractor requirements for the system design activities are described in Table 5 below.

Table 5, System Design Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 55.	The Contractor shall recommend specific methodologies for design and development activities prior to commencement of design or development activities for any customized components.	System Design Methodology
CR 56.	The Contractor shall work with the State on the completion of a detailed design of all license/permit types as defined in Appendix 2 – *Functional and Technical Requirements.*	Detailed Design Specifications
CR 57.	The Contractor shall develop and deliver a system architecture design document that describes the overall system architecture in terms of network, security, system, hardware, software, tools, peripherals, software licenses, and the logical distribution of system components and processes across the architecture.	System Architecture Design
CR 58.	During System Design, the Contractor shall deliver system security design documentation describing the logical security architecture design, the physical security architecture design, and the design of all controls to be used to mitigate threats to the confidentiality, integrity and availability of the System and system data.	System Security Design
CR 59.	The Contractor shall identify and document the database schemas, file formats, data views, an entity relationship diagram, and data dictionary for the System.	Database Documentation

Contractor Requirements		
	Task	**Deliverable or Process**
CR 60.	The Contractor shall deliver comprehensive data model documentation that clearly describes the conceptual, logical, and physical data characteristics of the System.	Data Model Documentation
CR 61.	The technical documentation shall include: • Anticipated data volume estimates; • Data needs for the system environment; • Updated data mapping; • Other interface descriptions; • Configuration report (that describes how each area of the licensing business is configured in the software); • Detailed specifications for hardware and software components; • System performance expectations; • Input on the State's cleansing and loading historical data as well as population of new data; and • Deployment plans.	Technical Documentation
CR 62.	The Contractor shall work with TDA to generate a detailed test plan defining: • The overall strategy for validating the functionality of the System; • The approach to ensure test coverage of each requirement; • The criteria for acceptance of each test; • The individual test cases that will be performed to execute the testing strategy; • The environments in which the tests will be conducted and data sources; and • The defect reporting and tracking tools for use by all agencies.	Test Plans
CR 63.	The test plans shall include: • Testing objectives; • Scope of testing (both what is in and what is out of scope); • Roles and responsibilities for test team members (who will be performing the test); • Testing approach; • Testing sequence; and • Defect reporting and criteria.	Test Plans
CR 64.	The test case descriptions shall be traced to requirements and include: • Test data needed to execute the tests; • Preconditions required prior to the start of test; • Criteria for suspending and resuming testing; and • Expected test results.	Test Plans

System Development

The System Development phase consists of all activities required to configure, customize, test, and validate the new system to the point at which it can be turned over for System Acceptance. This includes configuration and any required customization of all components of the System, including utilities required to adequately prepare and load the data. The Contractor will have to work with TDA to lay out a plan for developing and implementing the system. In addition, System Development consists of a series of tests of the system components, with each set of tests being performed against a progressively larger grouping of components until the full operation of the System has been verified. Actual test results will be documented and necessary corrective actions will be implemented in the System and system documentation. Status reports of testing progress will be provided on a regular basis

and will include the status of corrective actions. Since the ultimate goal of this activity is to produce a system that is ready for acceptance testing, an aspect of this phase is the creation of the various training materials and system documentation that support the new system, including preparation of help desk support and delivery of initial training. These materials need to address both the use and maintenance of the System and will play an integral part in the System Acceptance and System Implementation phases of the lifecycle. Deliverable requirements for the System Development activities are described in the table below.

Table 6, System Development Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 65.	The Contractor shall provide a system development methodology to support the software lifecycle that includes, but is not limited to, the use of commercially available system design and development tools.	System Development Methodology
CR 66.	The Contractor shall deliver a Requirements Traceability Matrix that identifies where and how each requirement has been addressed in the System.	Requirements Traceability Matrix
CR 67.	The Contractor shall utilize an industry standard testing methodology, to include unit testing, systems and integration testing, and user acceptance testing (functional, performance and reliability).	Test Methodology
CR 68.	The Contractor shall deliver test results including detailed outcomes for the following: • Data migration tests; • System tests (including performance tests); and • Security tests.	Test Results
CR 69.	The Contractor shall deliver test progress reports that include: • Number of defects identified in testing; • Types of defects found; and • Status of corrective actions.	Test Progress Reports
CR 70.	The Contractor shall update and deliver technical documentation to include corrective actions implemented as a result of testing activities.	Updated Technical Documentation
CR 71.	The Contractor shall update and deliver updated technical documentation including customization, system parameters, and configuration instructions.	Updated Technical Documentation
CR 72.	The Contractor shall develop and deliver the following user documentation that must be reflective of any specific configurations and customizations: • User Manual that will include instructions regarding the procedures the end-user would utilize to operate all modules of the System; • Database Administrator Manual, including installation and upgrade guides (this manual must address database refreshes); • System Administrator Manual; • System Operating Manual that will provide instructions regarding the phases, steps, and/or processes needed to operate the application and system software, including but not limited to application set up, user ID management, database maintenance and tuning, database and application recovery, and systems backup and recovery; • Frequently Asked Questions (FAQ) and scripts for help desk and technical support staff; • Documentation on how to incorporate customizations during system upgrades; and • Documentation on how to copy configuration and/or data to a new environment.	User Documentation
CR 73.	The user manuals shall include a collection of printable online documentation designed to instruct users in the operation of the System.	User Documentation

Contractor Requirements		
	Task	**Deliverable or Process**
CR 74.	The Contractor shall develop and deliver user training materials that provide instructions on the use of the System for all user roles, including any specific configurations and customizations.	Training Materials

System Acceptance

System Acceptance is the period in the project management lifecycle at which every aspect of the application being developed, along with any supporting data conversion routines and system utilities are thoroughly validated by TDA prior to proceeding with System Implementation. The System Acceptance phase is centered on gaining sufficient evidence of the System's accuracy and functionality to be able to proceed to System Implementation with the highest level of confidence possible in the success of the System. With the testing roadmap established in earlier lifecycle phases, the TDA will take responsibility for maneuvering the System through its operations. In addition to confirming the operation of the System and its fit to the business needs that it is intended to satisfy, System Acceptance is also the point in the lifecycle during which all supporting documentation and reference materials are refined and updated to guarantee their consistency with the final delivered system. Contractor Deliverable requirements for the System Acceptance activities are described in the table below.

Table 7, System Acceptance Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 75.	The Contractor shall deliver an updated Requirements Traceability Matrix that identifies where each requirement has been tested and the results of those tests.	Requirements Traceability Matrix
CR 76.	The Contractor shall deliver test results for the following: • Data validation results; • Data migration approach assistance • Acceptance test results (including performance tests); Security and vulnerability test results; and • Regression test results that re-test functions implemented in previous phases, to ensure the current phase implementation does not cause them to fail.	Test Results
CR 77.	The Contractor shall support acceptance testing to include both field testing for Point of Sale functions and user testing by the State.	Test Plans
CR 78.	The Contractor shall perform field testing for applicable staff TDA identifies for a time period of at least one month in an environment that has satisfactorily completed system/integration testing.	Test Plans
CR 79.	Acceptance of the System or system components will be contingent upon successful completion of acceptance testing as defined in any applicable Acceptance Test Plan as well as review and approval by the State of any other acceptance criteria as defined in the Acceptance Management Plan. The Contractor shall submit all project Deliverables through the acceptance management process developed and approved by the State during System Initiation.	Test Results
CR 80.	The Contractor shall identify the quality control (QC) measures and practices that will be implemented to ensure that the application is rigorously tested prior to implementation in production and is continuously monitored during the Project Period and System Warranty.	Test Plans

Contractor Requirements		
	Task	**Deliverable or Process**
CR 81.	The Contractor shall provide comprehensive performance testing, prior to cutover, that demonstrates the processing and response times of critical functions and transactions under various operational conditions (e.g., scenario scripts and system load and stress).	Test Results
CR 82.	The Contractor shall compile test data and provide test results within the time period specified in the Test Plan.	Test Results
CR 83.	The Contractor shall license testing tools for use by the State.	Testing Tools
CR 84.	The Contractor shall provide a classification and tracking method for system or application errors during acceptance testing that describes the severity of deficiency, and determination, based upon severity, of whether that error must be corrected prior to User Acceptance.	Issue Tracking System
CR 85.	The Contractor shall deliver an accepted system.	Accepted System
CR 86.	The Contractor shall deliver accepted migrated data in the System.	Migrated Data
CR 87.	The Contractor shall refine and deliver the following user documentation: • User Manual; • Database Administrator Manual, including installation and upgrade guides; • System Administrator Manual; • System Support Plan describing how to maintain the system configurations and customizations; • FAQs and scripts for help desk and technical support staff; • Documentation on how to incorporate customizations during system upgrades; and • Guide to standard reports.	Updated Technical Documentation
CR 88.	The Contractor shall deliver system security documentation describing the logical security architecture, the physical security architecture, and all controls that are used to mitigate threats to the confidentiality, integrity, and availability of the System and system data.	System Security Documentation
CR 89.	The Contractor shall refine and deliver training materials for all user roles.	Training Materials

System Implementation

The purpose of System Implementation can be summarized as the deployment and the transition of system support responsibilities. At a finer level of detail, deploying the System consists of executing all steps necessary to educate the system users on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the System are functioning properly. Deliverable requirements for the System Implementation activities are described in the table below.

Table 8, System Implementation Phase Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 90.	The Contractor shall deliver an operational system to the TDA that fulfills all system requirements.	Operational System
CR 91.	The Contractor shall deliver approved installation and data migration scripts to the TDA to promote the System to the appropriate database environments.	Data Migration Scripts
CR 92.	The Contractor shall take into account available windows of opportunity (due to annual processes and ongoing business operations) when determining the deployment timing of various functionality.	Installation and Deployment

Contractor Requirements		
	Task	**Deliverable or Process**
CR 93.	The Contractor must allow for flexible enforcement of the business rules during the implementation year where there will be item sales in both the current and new automated sales environments.	Installation and Deployment
CR 94.	Following the implementation of any system phase or component, the State, with assistance from the Contractor, shall monitor the production system to verify performance in accordance with all requirements and acceptance criteria for a period set forth in the Acceptance Management Plan and any applicable Acceptance Test Plans. Such monitoring will be conducted on-site and the Contractor shall provide all necessary resources to correct any defects promptly according to Service Levels identified in the *Pro Forma* Contract, Section A.67 – Support.	Production Verification Testing
CR 95.	The Contractor shall provide documentation and training to support the process of defect tracking and corrective action.	Issue Tracking Documentation
CR 96.	The Contractor shall be responsive to State staff operating the State's Help Desk when access to system support or technical assistance is requested or required.	Support for State Help Desk
CR 97.	The Contractor shall implement the System in the production environment in accordance with the approved Project Implementation and Transition Plan.	Implementation and Transition Assistance
CR 98.	The Contractor shall conduct knowledge transfer in accordance with the approved project knowledge transfer approach.	Knowledge Transfer
CR 99.	The Contractor shall provide the TDA with the software release schedule for the software components contained within the System.	Software Release Schedule

Training Requirements

The proposed system will be a complex system that will be used daily by TDA staff. The State considers the training of these users to be critical for acceptance of the System as well as the daily use of the System. The System project team will review and approve all Contractor System training staff and user training materials, including training plans and role-based training materials.

The project team training responsibilities include:

- Review and approval of all role-based System training schedules.
- Review and approval of all Contractor training staff.
- Review and approval of the overall System training plan.
- Identify all staff to be trained during the implementation by role.
- Review and approval of all Contractor-developed role-based System training materials.
- Provide training facilities, computers, and network connections for all of the System training sessions.
- Designate a training environment for use during training.
- Coordinate training activities with the State's Learning Management System as appropriate.

The TDA Staff Training Requirements are described in the table below.

Table 9, TDA Staff Training Requirements

Contractor Requirements		
	Task	**Deliverable or Process**
CR 100.	The Contractor shall provide all training materials (to include training curriculum/syllabus, training objectives etc.) for the training sessions.	Training Materials

Contractor Requirements		
	Task	**Deliverable or Process**
CR 101.	The Contractor shall provide training materials (in electronic format in a form acceptable to the State) to the State for approval at least 15 days prior to the training.	Training Materials
CR 102.	Training sessions will occur at least 30-60 days before the system implementation.	Training Sessions
CR 103.	The Contractor shall provide assistance to the TDA to implement a training environment in the designated technical environments.	Training Database
CR 104.	The Contractor shall provide the capability to refresh the System training environment for each training session.	Training Database
CR 105.	The Contractor shall develop the training data based on Participating Agency input and/or migrated/converted data.	Training Database
CR 106.	The Contractor shall provide training session attendance records to TDA.	Training Attendance Records
CR 107.	The Contractor shall provide web-based ad hoc training for self-study users.	Web-based Training
CR 108.	The Contractor shall perform a training needs analysis that identifies: • Critical training focus areas; • Role-based training modules; and • Role-based training media.	Training Needs Analysis
CR 109.	The Contractor shall refine and deliver a training plan identifying: • Schedule for all role-based training sessions; • Training evaluation collection, analysis, and improvement process; • Success metrics identification, collection, and evaluation process; • Expected training results; and • Post Training Support.	Training Plan
CR 110.	The Contractor shall develop customized TDA project role-based training for each role. Role-based training materials may include: • Participant Guidebooks (Printed [defined number by TDA] and Electronic) including exercises; • Instructor Guidebooks (Printed and Electronic) including exercises and answers; • PowerPoint Presentations; • User Manuals; and • Online Help.	Training Materials
CR 111.	The Contractor shall develop step-by-step instructions for adding a new license/permit type that will allow State staff to implement new license types without Contractor assistance.	Instructions for adding license types
CR 112.	The Contractor shall plan, organize, staff, direct, and control the training and development activities to meet the organizational and training goals of the project.	Training Sessions
CR 113.	The Contractor shall manage the training program, report all activities, and schedule all activities.	Training Sessions
CR 114.	The Contractor shall plan and perform training sessions in the TDA training locations indicated in the Staff Training Estimates table (Table 5). The Contractor will provide any specialized computer equipment (i.e. equipment other than a PC, projector or printer).	Training Sessions
CR 115.	The Contractor shall provide approved training staff for each System training session.	Training Session Staff
CR 116.	The Contractor shall coordinate with the TDA to schedule the role-based training prior to system implementation.	Role Based Training Sessions
CR 117.	The Contractor shall update all System training schedules to address any State comments.	Training Sessions

Contractor Requirements		
	Task	**Deliverable or Process**
CR 118.	The Contractor shall provide a mechanism for collecting training session evaluations (e.g. web-based survey tool)	Training Materials
CR 119.	The Contractor shall provide coaching and mentoring support for training session attendees for the implementation.	Coaching and Mentoring Support
CR 120.	The Contractor shall develop FAQ to document coaching requests and the provided responses to participating System users	Coaching and Mentoring Support
CR 121.	The Contractor shall update training material to clarify areas where repetitive coaching questions are received.	Training Materials
CR 122.	The Contractor shall develop Help Desk Diagnostic Scripts to aid Help Desk Personnel in diagnosing problems.	Diagnostic Scripts
CR 123.	The Contractor shall provide mentoring scripts for the Help Desk to follow in order to provide mentoring support after the Contractor mentoring support ends.	Mentoring Scripts
CR 124.	During Implementation, the Contractor shall coach and mentor TDA staff, enabling their ability to support and maintain the System.	Coaching and Mentoring Support
CR 125.	The Contractor shall update impacted training material whenever software changes, including customizations, affect the operation of the software.	Training Materials
CR 126.	The Contractor shall provide technical training for staff who will take over the administration of the System once in production. The Contractor shall provide training to State technical staff, including but not limited to: • Database structure and design; • System and application architecture; • Query development; and • Report development.	Technical Training Sessions
CR 127.	The Contractor shall provide training to State test staff on the testing procedures outlined in Section A.17 - Training Requirement.	Test Procedure Training Sessions
CR 128.	The Contractor will provide TDA a “Train-the-Trainer” approach that will allow key State staff to acquire the knowledge of the System necessary to be able to deliver End-user Training.	Train the Trainer Approach & Materials

The table below presents estimates of the numbers of users that will need to receive in depth training on the use or administration of the System.

Table 10, TDA Staff Training Estimates

Training Locations

Level	Training Description	Training Location	Total Number of Attendees
1	System Administrator Training	Nashville, TN – TDA Office	Minimum of 2
2	Account Administrator Training	Nashville, TN – TDA Office	Minimum of 2
3	Train the Trainer	Nashville, TN – TDA Office	Minimum of 5
4	General End User Training	Initial training shall be conducted in Nashville, TN.	Minimum of 10

Table 11, Maintenance and Support

Contractor Requirements		
	Task	**Deliverable or Process**
CR 129.	The software provider shall provide a System Support Plan that documents the detailed support procedures, including request initiation, prioritization, problem resolution, escalation, tool usage, organization and individual roles and responsibilities, and reporting requirements.	Maintenance & Support
CR 130.	The software provider shall provide Maintenance and Support in accordance with the Maintenance and Support Plan that results from this procurement, with services beginning immediately following the System Warranty period. At a minimum, the Maintenance and Support agreement will address the following: • Software issue resolution; • Access to Contractor Issue Tracking System for the State System support team; • Service Levels; • Software upgrades; • Technical assistance for the State System support team in the installation and regression testing of software upgrades; • Updates to user, technical, and training documentation to support software changes resulting from fixes or upgrades; • Remote diagnostics; and • On-site issue resolution if necessary.	Maintenance & Support
CR 131.	The software provider shall provide software maintenance and support for TDA staff members in accordance with agreed upon Service Levels.	Maintenance & Support
CR 132.	The software provider shall attend software support status meetings with TDA personnel as needed.	Maintenance & Support
CR 133.	The software provider shall provide recommendations on upgrading to new releases of the Software.	Maintenance & Support
CR 134.	The software provider shall maintain a software upgrade plan that will handle system customizations with minimal effort required by the State.	Maintenance & Support
CR 135.	The software provider shall prepare a rollback plan, mutually agreed to by the State, prior to any migration of any new releases of the Software or patches to the Software to the production environment.	Maintenance & Support
CR 136.	The software provider shall advise the State in writing within ten (10) days of notice from the State of a proposal to change software used in conjunction with the System, or at such later date as agreed to by the State.	Maintenance & Support
CR 137.	The software provider shall advise the State in writing whether the proposed replacement software is compatible with the System so that the System shall continue to operate at the same (or higher) level of performance as was achieved at the time of Final Acceptance. In the event the software provider advises the State that the proposed replacement software does not satisfy the requirements set forth here, the software provider shall, in its response to the State, recommend alternatives to the proposed replacement software, and, if necessary, modifications to the existing software and system that will satisfy such requirements. Examples of software that the State may change include, but are not limited to the database, operating system, web browser, or word processor.	Maintenance & Support

Table 12, System Support and System Warranty

Contractor Requirements		
	Task	**Deliverable or Process**
CR 138.	The Contractor shall provide a System Support Plan that documents the detailed support procedures, including request initiation, prioritization, problem resolution, escalation, tool usage, organization and individual roles and responsibilities, and reporting requirements.	System Support Plan
CR 139.	The Contractor shall provide System Support beginning at the first Implementation Stage through the Retainage Period. At a minimum, the System support plan will address the following: • Software issue resolution; • Access to Contractor Issue Tracking System for the System support team; • Service Levels; • Software upgrades; • Installation and regression testing of software upgrades; • Updates to user, technical, and training documentation to support software changes resulting from fixes or upgrades; • Remote diagnostics; and • On-site issue resolution if necessary.	System Support & System Warranty
CR 140.	Commencing from User Acceptance of the first Implementation Stage through the Retainage Period, the Contractor shall warrant the following: • Components or Deliverables specified and furnished by or through the Contractor in the course of providing the services described in the Agreement shall, individually and together, operate in accordance with all Acceptance Criteria for such Deliverables and the System and shall operate substantially uninterrupted and error-free, and be guaranteed against faulty material and workmanship. • Defects in the materials or workmanship of components or Deliverables specified and furnished by or through Contractor shall be promptly repaired or replaced by Contractor at no cost or expense to the State. • Accepted Deliverables and the System as a whole shall (i) continue to meet the functional, performance and reliability requirements of the State, as set forth in the RFQ and the resulting Agreement and the manufacturers' specifications for the Equipment and Software, as the same may be amended and updated and (ii) operate in conformance with the acceptance criteria established for each Deliverable, the System as a whole, and by the Acceptance Management Plan.	System Support & System Warranty
CR 141.	Commencing from User Acceptance of the first Implementation Stage through the Retainage Period, the Contractor shall promptly provide all necessary services and support at no cost to the State to ensure all Deliverables and the System operate in accordance with the warranties set forth in Table 11 above.	System Support & System Warranty
CR 142.	Commencing upon the completion of the Retainage Period, the system shall enter the Warranty phase, as defined in the *Pro Forma* Contract, Section A.18.	System Support & System Warranty

Contractor Requirements		
	Task	**Deliverable or Process**
CR 143.	Where the Contractor or other third-party manufacturer / developer markets any project Deliverable delivered by or through Contractor with a standard commercial warranty, such standard warranty shall be in addition to, and not relieve the Contractor from, the Contractor's obligations for System Support described herein. Where such standard commercial warranty covers all or some of the Project Period, Contractor shall be responsible for the coordination with other third-party Product manufacturer(s) / developer(s) for warranty repair or replacement of other third-party manufacturer's / developer's Product.	System Support & System Warranty
CR 144.	Where the Contractor or other third-party Product manufacturer(s) / developer(s) market any Project Deliverable with a standard commercial warranty which goes beyond the Project Period, the Contractor shall notify the State and pass through the manufacturer's standard commercial warranty to the State at no additional charge.	System Support & System Warranty
CR 145.	The Contractor shall provide the TDA staff members with access to a bug-reporting and enhancement-tracking system.	System Support & System Warranty
CR 146.	The Contractor shall provide technical and application support for TDA staff members in accordance with agreed upon Service Levels.	System Support & System Warranty
CR 147.	The Contractor shall attend software support status meetings with TDA personnel as needed.	System Support & System Warranty
CR 148.	The Contractor shall provide recommendations on upgrading to new releases of the Software.	System Support & System Warranty
CR 149.	The Contractor shall devise a software upgrade plan that will handle TDA customizations with minimal effort required by the State.	System Support & System Warranty
CR 150.	The Contractor shall prepare a rollback plan, mutually agreed to by the State, prior to any migration of any new releases of the Software or patches to the Software to the production environment.	System Support & System Warranty
CR 151.	The Contractor shall advise the State in writing within ten (10) days' notice of a proposal to change software used in conjunction with the System, or at such later date as agreed to by the State. The software provider shall advise the State in writing whether the proposed replacement software is compatible with the System so that the System shall operate in conformance with the Acceptance Criteria for the System. In the event the software provider advises the State that the proposed replacement software does not satisfy the requirements set forth there, the software provider shall, in its response to the State, recommend alternatives to the proposed replacement software, and, if necessary, modifications to the existing software and system that will satisfy such requirements. Examples of software that the State may change include, but are not limited to the database, operating system, web browser, or word processor.	System Support & System Warranty
CR 152.	The State seeks a System Warranty as described in this section; the Contractor will continue to provide the same level of support as during the Project Period for the System during an anticipated twelve month period following the Final Acceptance of the System.	System Warranty

The State's Acceptable Use Policy and Acceptance Use Agreement begins on next page.

STATE OF TENNESSEE

Administrative User Policy
Network, Data and Information Resource Access Rights and Obligations

Purpose
To ensure that individuals who are in a position of trust and/or operate information systems with elevated privileges understand his/her rights, responsibilities, obligations and consequences of misuse.

References:
Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994.
Tennessee Code Annotated, Section 10-7-504, effective July 1, 2001.
State of Tennessee Security Policies.

Objectives:
- Ensure the protection of proprietary, confidential, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
- Ensure that individuals who are granted escalated system and/or network resource privileges do not abuse such privileges for personal gain.
- Ensure that individuals do not take actions that result in obtaining money, knowledge, property, or an advantage to which those individuals are not entitled.
- Ensure that individuals do not intentionally, wrongfully, or improperly use or destroy State information resources, or conduct improper practices not limited to prosecutable fraud.
- Maintain security of and access to networked data and information resources on an authorized and trusted basis.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users granted administrative and/or privileged rights of his/her network access rights and obligations.

Scope
This Administrative User Policy applies to all individuals who have been provided administrative access rights to the State of Tennessee networks, State provided email, and/or Internet via agency issued network or system User ID's or physical access to such resources. The scope does not include State phone systems, fax machines, copiers, State issued cell phones or pagers unless those services are delivered over the State's IP network.

Network, Data and Information Resources Usage
State employees, vendors, business partners or subrecipients, local governments, and other governmental agencies may be authorized to access state network, data or information resources to perform business functions with or on behalf of the State. Users granted administrative rights must be acting within the scope of his/her employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature.

Network, Data and Information Resources Prohibitions

- Accessing, viewing, copying, sending, sharing and/or selling any information that is confidential by law, rule or regulation, or not otherwise available, without proper authorization.
- Leaving workstation(s) unattended without logging off or engaging password protection for the privileged account for which the user is responsible.
- Utilizing unauthorized, unlicensed, hacked, cracked or stolen software on computing platforms which could subject privileged accounts to further risk.
- Using network, data or information resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing network, data or information resources for activities that violate conduct policies established by the Information Systems Council (ISC), the Department of Human Resources, The Department of Finance and Administration, the Office for Information Resources and/or the Agency where the user is employed or under contract.
- Using escalated privileges to remove audit trails, system log files and/or security event logs in an effort to hide any data that would provide evidence supporting a violation of this policy.

Statement of Consequences

Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's information technology operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Statement of Enforcement

Noncompliance with this policy may result in the following actions:

1. Written notification will be sent to the Agency Head and to designated points of contact in the User Agency's Human Resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance issue. In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
2. Administrator user access credentials may be terminated immediately, and the individual may be subject to subsequent review. These actions may be grounds for disciplinary action up to and including dismissal as determined by the Agency Head.

STATE OF TENNESSEE

Administrator User Policy
Network, Data and Information Resource Access Rights and Obligations
User Agreement Acknowledgement

As an administrative or privileged user of State of Tennessee network, data or information resources, I agree to abide by the Administrator User Network, Data and Information Resource Access Rights and Obligations Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State confidential data, facilities and systems entrusted to me against unauthorized disclosure and/or use.
2. I will maintain all network, data and/or computer access credentials assigned to me in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
3. I will be accountable for all transactions performed using my computer access credentials.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.
5. I have read and agree to abide by the Data Center Processing Physical Security Policies that are in effect on the data of my signature below.
6. I agree to report any suspicious network, data and/or computer activity, security breach or violation of this policy to my supervisor.
7. Upon the termination of my employment or contractual relationship with the State of Tennessee, I will not disclose any proprietary, confidential, privileged, or otherwise sensitive data and resources.

Privacy Expectations
The State of Tennessee actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. These communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving administrative and/or privileged access to State of Tennessee data and information resources.

I understand the willful violation or disregard of any of these guidelines, statute or policies may result in my loss of access and disciplinary action, up to and including my dismissal, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Tennessee Personal and Commercial Computer Act of 2003 as cited at TCA 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

_____	_____
Type or Print Name	Edison ID
_____	_____
Signature	Date

REQUEST FOR CONFIDENTIAL DOCUMENTS

In order to receive the confidential documents described in Section 1.4 of the RFP, the State must receive a Notice of Intent to Propose (filed separately) and a signature on the attached Confidentiality Agreement by an officer of the prospective respondent who is authorized to bind the company.

NON-DISCLOSURE AGREEMENT (NDA)

_____, a Prospective Respondent on a procurement with the State of Tennessee (hereinafter "Prospective Respondent"), will be provided with copies of the following documents for the purposes of preparing a response to this procurement.

1. Edison Business Partner Interfaces – Technical Quick Start Guide

2. Enterprise Technology Architecture Standard Products

In consideration for access to these documents, Prospective Respondent agrees as follows:

1. These documents are confidential and proprietary and are not public records of the State of Tennessee.

2. These documents, or copies thereof, will only be disclosed to authorized employees and contractors of Prospective Respondent who need access to them for the purpose of preparing a response to the procurement. All individuals entrusted with these documents, or the information contained therein, will be notified of the confidentiality restrictions.

3. Prospective Respondent will maintain reasonable security procedures to protect paper and electronic copies of these documents.

4. If Prospective Respondent chooses not to offer a response or if the response does not result in a contract with the State, the Prospective Respondent will destroy all copies of the documents within a reasonable time. If requested by the State, Prospective Respondent will certify in writing that the confidential documents were destroyed.

5. If Prospective Respondent enters into a contract with the State based on this procurement, this confidentiality agreement will expire upon signature of the contract, and the confidentiality provisions of the contract will control.

6. Prospective Respondent agrees that unauthorized release of the documents would cause such harm to the State that injunctive relief would be an appropriate remedy. If any court rules that Prospective Respondent has breached this confidentiality agreement, Prospective Respondent shall reimburse the State for its cost of litigation, including attorney's fees, as well as any damages awarded by the court.

7. This confidentiality agreement shall be interpreted under the laws of the State of Tennessee.

_____
(signature)

_____
(name of company)

Signature of this document constitutes certification that the person signing the document has the authority to bind the company.

_____

for State of Tennessee

The *Public Enterprise Information Security Policies – v2.0* begins on next page.

Enterprise Information Security Policies

State of Tennessee
Department of Finance and Administration
Office for Information Resources
Information Security Program

Document Version 2.0 – December 22, 2014

Table of Contents

		Page
1.	EXECUTIVE SUMMARY	1
2.	INTRODUCTION	3
	Scope (2.1)	4
	Authority (2.2)	4
	Exceptions (2.3)	5
	Review (2.4)	5
	Document Format (2.5)	5
	Policy Maintenance (2.6)	6
3.	INFORMATION SECURITY POLICIES	7
	Management Direction for Information Security (3.1)	7
	Policies for Information Security (3.1.1)	7
	Policies for Information Security (3.1.2)	7
	Policies for Information Security (3.1.3)	7
4.	OPERATIONS SECURITY	8
	Operational Procedures and Responsibilities (4.1)	8
	Documented Operating Procedures (4.1.1)	8
	Change Management (4.1.2)	8
	Change Control Procedures (4.1.2.1)	8
	Capacity Management (4.1.3)	8
	Separation of Development, Testing and Operational Environments (4.1.4)	8
	Protection from Malware (4.2)	9
	Malicious Software Control (4.2.1)	9
	Backup (4.3)	9
	Data Backup (4.3.1)	9
	Logging and Monitoring 4.4)	9
	Event Logging (4.4.1)	9
	Availability and Performance Monitoring (4.4.2)	10
	Protection of Log Information (4.4.3)	10
	Administrator and Logs (4.4.4)	10
	Clock Synchronization (4.4.5)	10
	Control of Operational Software (4.5)	10
	Installation of Software on Operational Systems (4.5.1)	10
	Patch Management (4.5.1.1)	10
	Software Development Code (4.5.1.2)	11
	Review of Application and Operating System Changes (4.5.1.3)	11
	Technical and Vulnerability Management (4.6)	11
	Management of Technical Vulnerabilities (4.6.1)	11
	Restrictions on Software Installation (4.6.2)	11
	Information Systems Audit Considerations (4.7)	11
	Information Systems Audit Controls (4.7.1)	11

5. ACCESS CONTROL 12

Business Requirements of Access Control (5.1) 12
Access Control Policy (5.1.1) 12
Access to Networks and Network Services (5.1.2) 12
Remote Access (5.1.2.1) 12
Information Security Roles and Responsibilities (5.1.3) 12
Segregation of Duties (5.1.4) 12
User Access Management (5.2) 13
User Registration and De-Registration (5.2.1) 13
User Access Provisioning (5.2.2) 13
User Account Naming (5.2.2.1) 13
Management of Privileged Access Rights (5.2.3) 13
Management of Secret Authentication of Information Users (5.2.4) 13
Review of User Access Rights (5.2.5) 13
Removal or Adjustment of Access Rights (5.2.6) 14
User Responsibilities (5.3) 14
Use of Secret Authentication Information (5.3.1) 14
System and Application Access Control (5.4) 14
Information Access Restriction (5.4.1) 14
Secure Log-on Procedures (5.4.2) 14
System Administrator Access (5.4.2.1) 14
Logon Banner (5.4.2.2) 14
Service Account Use (5.4.2.3) 15
Password Management System (5.4.3) 15
Use of Privileged Utility Programs (5.4.4) 15
Access Control to Program Source Code (5.4.5) 15
Default Configurations (5.4.6) 15

6. ASSET MANAGEMENT 16

Responsibility for Assets (6.1) 16
Inventory of Assets (6.1.1) 16
Ownership of Assets (6.1.2) 16
Acceptable Use of Assets (6.1.3) 16
Return of Assets (6.1.4) 16
Asset Identification (6.1.5) 16
Data Classification (6.2) 16
Classification of Data (6.2.1) 17
Labelling of Data (6.2.2) 17
Handling and Use of Data (6.2.3) 17
Public Data Classification and Control (6.2.3.1) 17
Confidential Data Classification and Control (6.2.3.3) 17
Confidential Data on Personally Owned Devices (6.2.3.4) 17
Confidential Electronic Messages Classification and Control (6.2.3.5) 18
Payment Card Information Classification and Control (6.2.3.6) 18
Use of Confidential Data (6.2.3.7) 18
Media Handling (6.3) 19
Management of Removable Media (6.3.1) 19

Repair of Removable Media (6.3.1.1) 19
Disposal of Removable Media (6.3.2) 19
Physical Transfer of Removable Media (6.3.3) 19
Workstation Computing (6.4) 19
State Provided Workstation Computing Platforms (6.4.1) 19
Workstation Platform Reassignment (6.4.2) 20
Workstation Platform Disposal (6.4.3) 20
Cloud Services (6.4.4) 20

7. PHYSICAL AND ENVIRONMENTAL SECURITY 21

Secure Areas (7.1) 21
Physical Security Perimeter (7.1.1) 21
Physical Entry Controls (7.1.2) 21
Securing Offices, Rooms and Facilities (7.1.3) 21
Protecting against External and Environmental Threats (7.1.4) 21
Working in Secure Areas (7.1.5) 21
Delivery and Loading Areas (7.1.6) 21
Equipment (7.2) 22
Equipment Siting and Protection (7.2.1) 22
Supporting Utilities (7.2.2) 22
Cabling Security (7.2.3) 22
Equipment Maintenance (7.2.4) 22
Removal of Assets (7.2.5) 22
Security of Equipment and Assets Off-Premises (7.2.6) 22
Secure Disposal or Re-Use of Data Processing Equipment (7.2.7) 23
Unattended User Equipment (7.2.8) 23
Session Time Outs (7.2.8.1) 23
Clear Desk and Clear Screen Policy (7.2.9) 23

8. NETWORK CONNECTIVITY SECURITY 24

Network Security Management (8.1) 24
Network Controls (8.1.1) 24
Security of Network Services (8.1.2) 24
Segregation in Networks (8.1.3) 24
Information Transfer (8.2) 24
Information Transfer Policies and Procedures (8.2.1) 24
Agreements on Data Transfer Policies (8.2.2) 24
Electronic Messaging (8.2.3) 25
Internal Electronic Messages Control (8.2.3.1) 25
External Electronic Messages Control (8.2.3.2) 25
Electronic Messaging Management (8.2.3.3) 25
Confidentiality or Non-Disclosure Agreements (8.2.4) 25

9. MOBILE DEVICE SECURITY POLICY 26

Mobile Devices and Teleworking (9.1) 26
Mobile Device Policy (9.1.1) 26
Teleworking (9.1.2) 26

10. EXTERNAL PARTY SECURITY 27

Information Security for External Party Relationships (10.1) 27
Information Security Policy for External Party Relationships (10.1.1) 27
Identification of Risk (10.1.2) 27
Addressing Security within External Party Agreements (10.1.3) 27
Reporting of Security Incidents (10.1.3.1) 27
Sub-Contractors Requirements (10.1.3.2) 27
Addressing Security for Access to Citizen Data (10.1.4) 28

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE 29

Security Requirements of Information Systems (11.1) 29
Security Requirements of Information Systems (11.1.1) 29
Securing Application Services on Public Networks (11.1.2) 29
Protecting Application Services Transactions (11.1.3) 29
Information Security in Project Management (11.1.4) 29
Security in Development and Support Processes (11.2) 29
Security Requirements of Information Systems (11.2.1) 29
Security in Application Systems Development (11.2.1.1) 30
Input and Data Validation (11.2.1.2) 30
Output Data Validation (11.2.1.3) 30
Application Authorization (11.2.1.4) 30
Inter-process Message Authentication (11.2.1.5) 30
Control of Internal Processing (11.2.1.6) 30
System Change Control Procedures (11.2.2) 30
Technical Review of Applications after Operating Platform Changes (11.2.3) 30
Restrictions or Changes to Software Packages (11.2.4) 31
Secure System Engineering Principles (11.2.5) 31
Secure Development Environment (11.2.6) 31
Outsourced Development (11.2.7) 31
System Security Testing (11.2.8) 31
System Acceptance Testing (11.2.9) 31
Test Data (11.3) 31
Protection of Test Data (11.3.1) 31

12. BUSINESS CONTINUITY MANAGEMENT 32

Information Business Continuity (12.1) 32
Planning Information Systems Continuity (12.1.1) 32
Business Impact Analysis (12.1.1.1) 32
Critical Applications (12.1.1.2) 32
Non-Critical Applications (12.1.1.3) 32
Implementing Information Systems Continuity (12.1.2) 32
Verify, Review and Evaluate information Systems Continuity (12.1.3) 33
Redundancies (12.2) 33
Availability of Information Processing Facilities (12.2.1) 33

13. INFORMATION SECURITY INCIDENT MANAGEMENT 34

Management of Information Security Incidents and Improvements (13.1) 34
Responsibilities and Procedures (13.1.1) 34
Reporting Information Security Events (13.1.2) 34
Data Breach and Disclosure (13.1.2.1) 34
Reporting Information Security Weakness (13.1.3) 35
Assessment of and Decision on Information Security Events (13.1.4) 35
Response to Information Security Incidents (13.1.5) 35
Learning from Information Security Incidents (13.1.6) 35
Collection of Evidence (13.1.7) 35

14. CRYPTOGRAPHY 36

Cryptographic Controls (14.1) 36
Use of Cryptographic Controls (14.1.1) 36
Transmission Integrity (14.1.2) 36
Transmission Confidentiality (14.1.3) 36
Cryptographic Module Authentication (14.1.4) 36
Cryptographic Module Authentication (14.1.5) 37
Key Management (14.1.6) 37

15. COMPLIANCE 38

Compliance with Legal and Contractual Requirements (15.1) 38
Identification of Applicable Legislation and Contractual Requirements (15.1.1) 38
Intellectual Property Rights (15.1.2) 38
Protection of Records (15.1.3) 38
Privacy and Protection of Personally Identifiable Information (15.1.4) 38
Regulation of Cryptographic Controls (15.1.5) 38
Information Security Reviews (15.2) 39
Independent Review of Information Security (15.2.1) 39
Compliance with Security Policies and Standards (15.2.2) 39
Technical Compliance Review (15.2.3) 39

16. HUMAN RESOURCE 40

Prior to Employment (16.1) 40
Screening (16.1.1) 40
Acceptable Use Policy (16.1.2) 40
During Employment (16.2) 40
Management Responsibilities (16.2.1) 40
Information Security Awareness, Education and Training (16.2.2) 40

17. VERSION HISTORY 41

18. TERMS AND DEFINITIONS 42

1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the confidentiality, integrity and availability of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been created to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by, or operated on behalf of the State of Tennessee. The methodologies and practices of external entities that require access to the State of Tennessee's information resources may be impacted and could be included in this scope. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

This document applies to all full- and part-time employees of the State of Tennessee, all third parties, contractors or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency information technology (IT) professionals and approval by the Chief Information Security Officer (CISO) and executive management team within the Office for Information Resources, Department of Finance and Administration.

All information resources and any information system owned by the State of Tennessee should be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the State government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

All of the approved policies will support the requirements of the Information Systems Council of the State of Tennessee.

2. INTRODUCTION

The Information Security Challenge

Information technology (IT) solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and technologies that support business processes at a low cost is a foundational component of successful IT programs. This integration moves quickly to align itself with the "just in time" requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes bypassing existing processes to meet time demands of the customers whom they serve. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need to evaluate risk and has established information security programs. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy to list a few.

Security policies are a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 27002 standard framework. The policies are designed to comply with applicable statutes and regulations; however, if there is a conflict, applicable statutes and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment.

Scope (2.1)

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) controlled by or operated on behalf of the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

All full- and part-time employees of the State of Tennessee, all third parties, contractors, or vendors who work on state premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data should adhere to the policies and requirements set forth in this document.

Authority (2.2)

The Information Systems Council (ISC) has authorized the Department of Finance and Administration, Office for Information Resources (OIR) to establish and enforce enterprise policies and standards as they are related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. The Office for Information Resources is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

Reference:

Tennessee Code Annotated, Section 4-3-5501, effective, May 10, 1994
ISC Information Resource Policies, Policy 1.00
ISC Information Resource Policies, Policy 13.00

Exceptions (2.3)

All exceptions to any of the security policies will be reviewed, evaluated and processed by a member of the Chief Information Security Officer's staff.

Review (2.4)

Review of this document takes place within Security Advisory Council sessions and will occur on an annual basis at a minimum. Document review can also be requested by sending a request to the Chief Information Security Officer.

The official policy document and supporting documentation will be published on the OIR intranet site located at:

http://intranet.tn.gov/finance/oir/security/policy.html

Document Format (2.5)

This document generally follows the International Standards Organization (ISO) 27002 (2013) standard framework for information technology security management. Each section starts with a high-level security control category followed by the control objective. Policy statements follow the objectives.

The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise.

X. Section Name

Control Category (x.x)
Objective Statement

Policy Name (x.x.x)
Policy Statement

Sub-Policy Name (x.x.x.x)
Sub-Policy Statement

MINIMUM COMPLIANCE REQUIREMENTS:

Policy Maintenance (2.6)

All policies will be maintained in accordance with the OIR policy process documentation.

3. INFORMATION SECURITY POLICIES

Management Direction for Information Security (3.1)

Objective: To provide management direction and support for information security in accordance with agency business requirements and relevant state and federal statute and regulations for the State of Tennessee's computing environments.

Policies for Information Security (3.1.1)

OIR Information Security Management will initiate and control an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.

Policies for Information Security (3.1.2)

Agencies may develop agency specific policy documents as required by agency or regulatory requirement provided the minimum requirements set forth in this document are met.

Policies for Information Security (3.1.3)

Agencies are responsible for communicating this policy document throughout their respective agencies.

4. OPERATIONS SECURITY

Operational Procedures and Responsibilities (4.1)

Objective: To protect critical State information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction to ensure correct and proper operations.

Documented Operating Procedures (4.1.1)

All agencies of the State of Tennessee and vendors or contractors acting on behalf of the State should identify, document and maintain standard security operating procedures and configurations for their respective operating environments and ensure the documentation is available to all users who need it.

Change Management (4.1.2)

Changes to information processing facilities and systems should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to ensure satisfactory control of all changes to equipment, software, configurations or procedures that affect the security of the State of Tennessee's operational environment. All written documentation generated by the change control policies and procedures should be retained as evidence of compliance.

Change Control Procedures (4.1.2.1)

Change control procedures should include authorization, risk assessment, logging, audit ability, and roll back procedures.

Capacity Management (4.1.3)

The use of resources should be monitored and tuned so that projections of future capacity requirements can be made.

Separation of Development, Testing and Operational Environments (4.1.4)

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and should not be used in development or test environments.

Protection from Malware (4.2)
Objective: Prevent the automated propagation of malicious code and contamination of environments attached to the enterprise network.

Malicious Software Control (4.2.1)

All computing platforms that are attached to the State's enterprise technology infrastructure or operated on behalf of the State should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs and rootkits. Compromised systems should be removed from the operational environment. All computing platforms that are attached to the State's enterprise technology infrastructure will participate in the State's enterprise antivirus program if antivirus signatures are available for the computing platforms. OIR Security Management reserves the right to seize any compromised system for forensic analysis.

Backup (4.3)
Objective: To prevent loss of data and to ensure data availability.

Data Backup (4.3.1)

Backup copies of data, software and system images should be taken and tested regularly in accordance with established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and State policy. Results of restore tests should be furnished to data owners with recommendations for any remedial steps found. Data owners should approve any remedial plans and timelines for implementing those remediation steps within a reasonable period not to exceed three months. Following remediation, the restore testing should be repeated and results documented to ensure that those steps mitigated all identified issues.

Logging and Monitoring 4.4)
Objective: To record events and generate evidence.

Event Logging (4.4.1)

All systems should be configured to support security event logging, recording user activities, exceptions, faults and information security events. System administrators should monitor and report inappropriate access to the OIR Customer Care Center. Mission critical systems should be configured to support automated logging to a facility that protects the integrity of the logs. Logging levels and

monitored elements will be configured in accordance with federal and state statute and regulatory requirements.

Availability and Performance Monitoring (4.4.2)

Mission critical systems should be configured to support State approved automated monitoring of system availability and performance.

Protection of Log Information (4.4.3)

Logging facilities and log information should be protected against tampering and unauthorized access.

Administrator and Logs (4.4.4)

System administrator activities should be logged and the logs protected and regularly reviewed.

Clock Synchronization (4.4.5)

Approved State of Tennessee managed enterprise network time servers should be the only State devices permitted to synchronize with external time services. All State provided or managed systems will synchronize time with approved State of Tennessee managed enterprise network time servers. All non-State provided or managed systems storing, processing or transmitting State data should be synchronized to State approved time synchronization services.

Control of Operational Software (4.5)

Objective: To ensure the integrity of operational systems.

Installation of Software on Operational Systems (4.5.1)

Only software that has been licensed and approved as a State standard software product or that has been approved as an exception through the State's architecture standards approval process should be installed on devices covered by the software's license agreement.

Patch Management (4.5.1.1)

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable

date can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Software Development Code (4.5.1.2)

Software development code cannot be installed on production systems (i.e. non-compiled software programming code)

Review of Application and Operating System Changes (4.5.1.3)

Applications and operating systems should be reviewed and tested to ensure that there is no adverse impact on operations or security when a change has been performed on the operating system. (e.g. patch).

Technical and Vulnerability Management (4.6)
Objective: To prevent the exploitation of technical vulnerabilities.

Management of Technical Vulnerabilities (4.6.1)

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk to the State and appropriate measures implemented to address the associated risk.

Restrictions on Software Installation (4.6.2)

Users should not install software that has not been approved by OIR and their agency.

Information Systems Audit Considerations (4.7)
Objective: To minimize the impact of audit activities on operational systems.

Information Systems Audit Controls (4.7.1)

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

5. ACCESS CONTROL

Business Requirements of Access Control (5.1)

Objective: To limit access to information and information processing facilities.

Access Control Policy (5.1.1)

All access rules and requirements to access the State of Tennessee's information resources should be developed, documented and maintained by their respective resource owners. Access to the State of Tennessee's information resources will be granted consistent with the concept of least privilege. All information processing systems owned by or operated on behalf of the State of Tennessee should have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use.

Access to Networks and Network Services (5.1.2)

All access and connectivity to the State of Tennessee's enterprise network or networks operated on behalf of the State should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

Remote Access (5.1.2.1)

All users who are accessing the State's internal network should access those resources through a State approved site-to-site Virtual Private Network (VPN) connection or through a multifactor VPN solution. All users who access State data on networks operated on behalf of the State should use secure connection methods.

Information Security Roles and Responsibilities (5.1.3)

All information security responsibilities should be defined and assigned by the access granting authority.

Segregation of Duties (5.1.4)

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse of the State's assets.

User Access Management (5.2)

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

User Registration and De-Registration (5.2.1)

A formal user registration and de-registration process should be implemented to enable assignment of access rights and to adjust those rights as the user's role changes.

User Access Provisioning (5.2.2)

User access to information resources should be authorized and provisioned according to the Agency's employee provisioning process.

User Account Naming (5.2.2.1)

All State user accounts will follow a State approved standardized naming convention.

Management of Privileged Access Rights (5.2.3)

Users should have the least privileges required to perform their roles as identified and approved by their agency. The allocation and use of privileged access rights should be restricted and controlled.

Management of Secret Authentication of Information Users (5.2.4)

The allocation of secret authentication information should be controlled through a formal management process.

Review of User Access Rights (5.2.5)

A user's access rights should be reviewed, validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies).

Removal or Adjustment of Access Rights (5.2.6)

All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day.

User Responsibilities (5.3)

Objective: To make users accountable for safeguarding their authentication information.

Use of Secret Authentication Information (5.3.1)

Users should follow State policy in the use of secret authentication information.

System and Application Access Control (5.4)

Objective: To prevent unauthorized access to systems and applications.

Information Access Restriction (5.4.1)

Access to information and application system function should be restricted in accordance with the defined access control policy.

Secure Log-on Procedures (5.4.2)

Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

System Administrator Access (5.4.2.1)

All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in State managed data processing facilities or facilities operated on behalf of the State must use a multifactor VPN solution to obtain access.

Logon Banner (5.4.2.2)

All systems and devices owned and operated by or on behalf of the State of Tennessee must display the State approved logon banner before the user is able to log in.

Service Account Use (5.4.2.3)

Service accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

Password Management System (5.4.3)

Password management systems should be interactive and should ensure quality passwords.

Use of Privileged Utility Programs (5.4.4)

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Access Control to Program Source Code (5.4.5)

Access to program source code should be restricted to authorized users.

Default Configurations (5.4.6)

All applications and processing devices that are attached to the State's enterprise technology infrastructure should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.

6. ASSET MANAGEMENT

Responsibility for Assets (6.1)

Objective: To identify organizational assets and define appropriate protection responsibilities.

Inventory of Assets (6.1.1)

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be created and maintained in order to protect the assets.

Ownership of Assets (6.1.2)

All information resource assets listed in the asset inventory should have an assigned owner or entity who will ensure the assets are protected in a manner consistent with their value, sensitivity and criticality to the business and operation of the State's government and those it serves or as specified by any superseding state or federal statute or regulation**.**

Acceptable Use of Assets (6.1.3)

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented and communicated to the employees and contractors who have access to those assets.

Return of Assets (6.1.4)

All employees and contractors must return all state assets in their possession upon termination of their employment or contract**.**

Asset Identification (6.1.5)

All state hardware assets will be named in accordance with the State approved standardized naming convention.

Data Classification (6.2)

Objective: To ensure the data used and managed by the State receives an appropriate level of protection commensurate with the value, importance and criticality of the data to the State.

Classification of Data (6.2.1)

Data assets owned and/or managed by the State of Tennessee should be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable state and/or federal statute or regulations to indicate the need, priorities and degree of protection it will receive. At a minimum, data will be classified as Public or Confidential.

Labelling of Data (6.2.2)

An appropriate set of procedures for labeling data assets owned and/or managed by the State of Tennessee should be developed and implemented in accordance with the State's data classification scheme.

Handling and Use of Data (6.2.3)

Procedures for handling data assets should be developed and implemented in accordance with the data classification scheme adopted by the State.

Public Data Classification and Control (6.2.3.1)

Data classified as public should be protected from unauthorized modification or destruction.

Confidential Data Classification and Control (6.2.3.3)

Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and cannot be used in development or test environments or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity and criticality to the business and operation of state government. Data classified as confidential must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.

Confidential Data on Personally Owned Devices (6.2.3.4)

Confidential data should not be stored on personally owned computing platforms or on personally owned mobile computing platforms unless managed by the State's mobile device management solution.

Confidential Electronic Messages Classification and Control (6.2.3.5)

E-mail sent from the State's domain out through the public Internet must be encrypted if it contains confidential information in the body or attachment. Confidential information should not be placed into the subject line of the message.

Payment Card Information Classification and Control (6.2.3.6)

Payment card information must be considered confidential when an individual's first name or first initial and last name are present in combination with account number, credit or debit card number, required security code, access code, or password that would permit access to an individual's financial account. (Payment Card Industry Data Security Standard https://www.pcisecuritystandards.org/security_standards/)

The Payment Card Industry – Data Security Standards (PCI DSS) comprise a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector statutes and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional statutes, government regulations, or other legal requirements.

All payment card information stored and processed by the State, or transmitted over State networks must be in compliance with the PCI-DSS. Storage of the full Primary Account Number (PAN) on State systems is prohibited. Agencies that use payment card services should also comply with statewide accounting policies as documented by the Department of Finance and Administration, Division of Accounts.

Use of Confidential Data (6.2.3.7)

The use of confidential data will only be permitted in production systems. The use of confidential data is prohibited from training, test, and development systems.

To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities. Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible.

Media Handling (6.3)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on media.

Management of Removable Media (6.3.1)

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Repair of Removable Media (6.3.1.1)

Removable media should be sanitized prior to removing it from State facilities for maintenance or repair.

Disposal of Removable Media (6.3.2)

Removable media should be disposed of securely when no longer required, using approved State procedures.

Physical Transfer of Removable Media (6.3.3)

Removable media containing sensitive or confidential data must be protected against unauthorized access, misuse or corruption during transport.

Workstation Computing (6.4)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on user assigned processing devices.

State Provided Workstation Computing Platforms (6.4.1)

Workstation computing platforms, including laptops should be physically protected against theft when left unattended. Workstation computing platforms should not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a workstation computing platform should have approval from the

asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation should be encrypted while stored on the workstation computing platform.

Workstation Platform Reassignment (6.4.2)

All workstation computing platforms including all external storage devices should be sanitized prior to being re-issued or re-purposed to another employee.

Workstation Platform Disposal (6.4.3)

Hard drives in workstation computing platforms including all mobile storage devices should be sanitized using approved sanitization procedures or destroyed prior to transfer or surplus of processing device to non-State agencies.

Cloud Services (6.4.4)

Agencies and full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who are acting on behalf of the State who use cloud services for State business should seek OIR guidance and approval for proposed cloud solutions prior to enabling cloud services.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas (7.1)

Objective: To prevent unauthorized physical access, damage and interference to the State's information and information processing facilities.

Physical Security Perimeter (7.1.1)

All enterprise data processing facilities that process or store data classified as critical or sensitive should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Physical Entry Controls (7.1.2)

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

Securing Offices, Rooms and Facilities (7.1.3)

Physical security for offices, rooms and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

Protecting against External and Environmental Threats (7.1.4)

Physical protection against natural disaster, malicious attack or accidents should be considered and incorporated in facility design, construction and placement.

Working in Secure Areas (7.1.5)

Procedures for working in secure areas should be created and implemented.

Delivery and Loading Areas (7.1.6)

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

Equipment (7.2)

Objective: To prevent loss, damage, theft or compromise of assets or an interruption to State operations.

Equipment Siting and Protection (7.2.1)

Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Equipment located in areas where the State of Tennessee is unable to maintain a secure perimeter should be locked in a secured manner with access controlled by the State of Tennessee. Secured cabinets or facilities should support further segregation within the State of Tennessee's Information Technology (IT) organization based on role and responsibility.

Supporting Utilities (7.2.2)

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

Cabling Security (7.2.3)

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference or damage.

Equipment Maintenance (7.2.4)

Equipment should be correctly maintained to ensure its continued availability and integrity.

Removal of Assets (7.2.5)

All equipment, software or information that is a part of State operational systems or processes should not be taken off-site without the prior authorization from executive management or a designated representative and should be removed according to documented agency equipment transfer procedures.

Security of Equipment and Assets Off-Premises (7.2.6)

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)

All data processing equipment including storage devices subject to transfer or reuse should be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding state or federal requirements. Data processing equipment assets that are not subject to transfer or reuse should be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding state or federal requirements.

Unattended User Equipment (7.2.8)

Users should ensure that unattended data processing equipment has appropriate protection.

Session Time Outs (7.2.8.1)

All systems and devices owned and operated by or on behalf of the State of Tennessee should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

Clear Desk and Clear Screen Policy (7.2.9)

All data classified as confidential must be stored in a locked cabinet or room when unattended. All data processing equipment that provide access to Information Processing Systems will be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended.

All computing platforms residing in non-secured facilities with attached displays should be oriented away from direct line of sight from unauthorized viewers.

8. NETWORK CONNECTIVITY SECURITY

Network Security Management (8.1)

Objective: To ensure the protection of the State's assets that are accessible by suppliers and vendors.

Network Controls (8.1.1)

Networks should be managed and controlled to protect information in systems and applications.

Security of Network Services (8.1.2)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Segregation in Networks (8.1.3)

All enterprise network architectures operated by, or on behalf of, the State of Tennessee should be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones should be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the OIR Security Management Team.

Information Transfer (8.2)

Objective: To maintain the security of information transferred within network infrastructures manage by on behalf of the State and with any external entity.

Information Transfer Policies and Procedures (8.2.1)

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements on Data Transfer Policies (8.2.2)

Agreements should address the secure transfer of business information between the State and external parties.

Electronic Messaging (8.2.3)

Data involved in electronic messaging should be appropriately protected.

Internal Electronic Messages Control (8.2.3.1)

Email and instant messages internal to the State's domain containing confidential data should be encrypted during transmission. Confidential information should not be placed into the subject line of email or as any part of instant messages.

External Electronic Messages Control (8.2.3.2)

E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.

Electronic Messaging Management (8.2.3.3)

All electronic messages created, sent or received in conjunction with the transaction of official business should use the State approved gateway(s) to communicate via the Internet.

Confidentiality or Non-Disclosure Agreements (8.2.4)

When exchanging or sharing information classified as Sensitive or Confidential with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party.

Note: Agencies should work with agency legal counsel to ensure proper language is used.

9. MOBILE DEVICE SECURITY POLICY

Mobile Devices and Teleworking (9.1)

Objective: To ensure the security of teleworking and the use of mobile devices.

Mobile Device Policy (9.1.1)

All mobile devices that connect to State of Tennessee managed data or infrastructure should be managed by the State's enterprise mobile device management solution or the State's enterprise configuration manager and should comply with appropriate mobile device usage policies as required by state or federal statute or regulation.

Teleworking (9.1.2)

Teleworkers should comply with the appropriate telework policies as required by state or federal statute, regulation, state or agency policy.

10. EXTERNAL PARTY SECURITY

Information Security for External Party Relationships (10.1)

Objective: To ensure the protection of the State's assets that are accessed, processed, communicated to, or managed by external parties, suppliers or vendors. This includes any external party who has access to physical data processing facilities, logical access to State data processing systems via local or remote access or access via another external party into the State's data processing facilities.

Information Security Policy for External Party Relationships (10.1.1)

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the State's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, executive orders, standards, controls and regulations.

Identification of Risk (10.1.2)

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any State of Tennessee information, information technology asset or information process facility.

Addressing Security within External Party Agreements (10.1.3)

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for the State's processing systems or infrastructure.

Reporting of Security Incidents (10.1.3.1)

External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of State data immediately.

Sub-Contractors Requirements (10.1.3.2)

Primary external parties should require their sub-contractors to abide by State of Tennessee policies and security requirements, as applicable.

Addressing Security for Access to Citizen Data (10.1.4)

Risk involving external party access to citizen data should be identified and proper controls implemented prior to the granting of access to any State of Tennessee citizen data. Appropriate controls should be agreed upon, documented in external party agreements and implemented prior to the granting of access to any citizen data.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security Requirements of Information Systems (11.1)

Objective: To ensure that information security is an integral part of information systems throughout their life cycle. This includes application infrastructure, vendor applications, agency-developed, and user-developed applications and information systems which provide services over public networks or the State's internal network.

Security Requirements of Information Systems (11.1.1)

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance and disposal phases.

Securing Application Services on Public Networks (11.1.2)

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

Protecting Application Services Transactions (11.1.3)

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Information Security in Project Management (11.1.4)

Information security should be addressed at project initiation and throughout the lifecycle of the project.

Security in Development and Support Processes (11.2)

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

Security Requirements of Information Systems (11.2.1)

Requirements, rules and guidelines for the development of software and systems should be established and applied to all systems development.

Security in Application Systems Development (11.2.1.1)

Input validation, authentication, and authorization should be included in the design, development and implementation of applications.

Input and Data Validation (11.2.1.2)

Applications should not pass raw input to other processes including, but not limited to, other applications, web services, application server and databases. Applications should use parameterized queries or stored procedures, not dynamic SQL statements.

Output Data Validation (11.2.1.3)

Applications should not echo input back to the user or disclose information about the underlying system through error messages.

Application Authorization (11.2.1.4)

Applications that provide access to information in databases or from network shares should perform user authentication.

Inter-process Message Authentication (11.2.1.5)

Inter-process message authentication should be used to verify that a message originated from a trusted source and that the message has not been altered during transmission.

Control of Internal Processing (11.2.1.6)

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

System Change Control Procedures (11.2.2)

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Technical Review of Applications after Operating Platform Changes (11.2.3)

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Restrictions or Changes to Software Packages (11.2.4)

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

Secure System Engineering Principles (11.2.5)

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Secure Development Environment (11.2.6)

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development (11.2.7)

Outsourced system development should be monitored and supervised to ensure the State's policies and practices are followed and to ensure appropriate security controls are in place.

System Security Testing (11.2.8)

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release and prior to assigning public IP addresses or being moved or promoted into the production environment.

System Acceptance Testing (11.2.9)

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Test Data (11.3)

Objective: To ensure the protection of the data used for testing.

Protection of Test Data (11.3.1)

Test data should be selected carefully, protected and controlled. The use of production data for development and testing is prohibited.

12. BUSINESS CONTINUITY MANAGEMENT

Information Business Continuity (12.1)

Objective: To ensure the continued availability of business information and security enabled systems in the event of a crisis or disaster.

Planning Information Systems Continuity (12.1.1)

All State agencies should determine their requirements for information security and the continuity of information management systems in adverse situations, e.g. during a crisis or disaster.

Business Impact Analysis (12.1.1.1)

All State agencies should perform a Business Impact Analysis (BIA) to determine how the loss of their IT applications or information security systems would impact their business functioning and ability to deliver their core services to citizens, other agencies, and regulatory bodies.

Critical Applications (12.1.1.2)

Systems including Infrastructure components, applications and security systems identified as critical in the Business Impact Analysis will be recovered in accordance with the Business Impact Analysis and documented system recovery strategy.

Non-Critical Applications (12.1.1.3)

Infrastructure components and applications identified as non-critical in the Business Impact Analysis will be recovered on a best–effort basis. The components and applications listed as non-critical should have an explanation in the BIA justifying their low importance and demonstrating how the loss of their associated functionality will be acceptable during an event or how a manual workaround can be implemented.

Implementing Information Systems Continuity (12.1.2)

All State agencies should establish, document, implement and maintain processes, procedures and controls to ensure the required level of business continuity for all systems during an adverse situation.

Verify, Review and Evaluate information Systems Continuity (12.1.3)

All State agencies and vendors or contractors who operate on behalf of the State should verify the established and implemented information systems continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Redundancies (12.2)

Objective: To ensure availability of information processing facilities.

Availability of Information Processing Facilities (12.2.1)

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

13. INFORMATION SECURITY INCIDENT MANAGEMENT

Management of Information Security Incidents and Improvements (13.1)

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Responsibilities and Procedures (13.1.1)

The State of Tennessee will establish a Computer Security Incident Response Team (CSIRT). The CSIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The CSIRT members will be appointed based on their position and capabilities within the organization. Each agency should designate an information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC will have responsibility for incident escalations, actions and authority for the administrative oversight of security for the information technology resources under the agency's control. The POC within each agency will participate as a member of the CSIRT. The CISO of the State of Tennessee will appoint members from within OIR to participate in the CSIRT.

Reporting Information Security Events (13.1.2)

Information security events should be reported through appropriate channels using the Guidelines in the State of Tennessee Incident Response, Alerting and Communications Plan.

Data Breach and Disclosure (13.1.2.1)

Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties must provide notice of the disclosure in accordance with TCA 47-18-2107 or any other applicable state and/or federal statute or regulations).

Reporting Information Security Weakness (13.1.3)

Employees and contractors using the State's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the OIR Customer Care Center.

Assessment of and Decision on Information Security Events (13.1.4)

Information security events should be assessed and a determination made on whether to classify the event as an incident in accordance with the Incident Response Plan.

Response to Information Security Incidents (13.1.5)

Information security incidents will be managed in accordance with the documented procedures in the State of Tennessee Incident Response, Alerting and Communications Plan.

Learning from Information Security Incidents (13.1.6)

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Collection of Evidence (13.1.7)

The State should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

14. CRYPTOGRAPHY

Cryptographic Controls (14.1)

Objective: To ensure proper and effective use of cryptography to protect the confidentiality and integrity of data owned or managed by the State. Confidential information must be encrypted by the use of valid encryption processes for data at rest and in motion as required by state or federal statute or regulation. This includes but is not limited to sensitive information stored on mobile devices, removable drives and laptop computers.

Use of Cryptographic Controls (14.1.1)

Cryptographic controls should be based on the classification and criticality of the data. In deciding what strength and type of control to be deployed, both stand alone and enterprise level encryption solutions should be considered. Attention should be given to regulations, national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques.

Transmission Integrity (14.1.2)

Information systems should protect the integrity of transmitted information traveling across both internal and external communications. This control applies to communications across internal and external networks

Transmission Confidentiality (14.1.3)

Information systems should protect the confidentiality of transmitted information. The State will employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Cryptographic Module Authentication (14.1.4)

Information systems must use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal statutes, state statutes, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use will be compared to the list of NIST validated cryptographic modules quarterly to ensure compliance.

Cryptographic Module Authentication (14.1.5)

Information systems will obtain and issue public key and Secure Socket Layer (SSL) certificates from an approved service provider. This control focuses certificates with visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Key Management (14.1.6)

A secured environment should be established to protect the cryptographic keys used to encrypt and decrypt information. Cryptographic key management and establishment will be performed using automated mechanisms with supporting manual procedures. Keys should be securely distributed and stored. Access to keys should be restricted only to individuals who have a business need to access them. All access to cryptographic keys requires authorization and should be documented. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

15. COMPLIANCE

Compliance with Legal and Contractual Requirements (15.1)

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Identification of Applicable Legislation and Contractual Requirements (15.1.1)

All relevant legislative, statutory, regulatory, contractual requirements and the State's approach to meet these requirements should be explicitly identified, documented and kept current for each information system, each agency and each entity that stores, processes or transmits data on behalf of the State.

Intellectual Property Rights (15.1.2)

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products.

Protection of Records (15.1.3)

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with state or federal statutory, regulatory, contractual and business requirements.

Privacy and Protection of Personally Identifiable Information (15.1.4)

The privacy and protection of personally identifiable information should be ensured as required by relevant federal or state statute or regulation.

Regulation of Cryptographic Controls (15.1.5)

Cryptographic controls should be used in compliance with state or federal statutory, regulatory, contractual and business requirements.

Information Security Reviews (15.2)

Objective: To ensure that information security is implemented and operated in accordance the organizational policies and procedures.

Independent Review of Information Security (15.2.1)

The State's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently and at planned intervals or when significant changes occur.

Compliance with Security Policies and Standards (15.2.2)

Managers should regularly review the compliance of information processing and procedures within their area of responsibility for accuracy and applicability with the appropriate security policies, standards and any other security requirements.

Technical Compliance Review (15.2.3)

Information systems should be regularly reviewed for compliance with the State's information security policies and standards.

16. HUMAN RESOURCE

Prior to Employment (16.1)

Objective: To ensure all full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors understand their responsibilities in regards to information security requirements for the State of Tennessee's computing environments.

Screening (16.1.1)

Background and verification checks on all candidates for employment should be conducted in accordance with relevant statutes and published state policies.

Acceptable Use Policy (16.1.2)

All agencies should ensure that their full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who use State of Tennessee resources have read and accept the terms of the relevant State's Acceptable Use Policies. Proof of employee acceptance and acknowledgement will be maintained by the agency.

During Employment (16.2)

Objective: To ensure employees and contractors are aware of and fulfill their information security responsibilities.

Management Responsibilities (16.2.1)

Management should ensure that all employees and contractors are aware of and fulfill their information security responsibilities.

Information Security Awareness, Education and Training (16.2.2)

All State employees who have access to State systems and where relevant, contractors should utilize State-provided security awareness education and training when first employed and at least annually thereafter.

17. VERSION HISTORY

18. TERMS AND DEFINITIONS

Access Credentials - Access Credentials are issued to users to provide access to particular data or resources. Examples include passwords, badges, and card keys for doors.

Access Granting Authority – The access granting authority is the individual or group that has the responsibility for determining appropriate access and use of resources.

Asset – An asset is anything that can be considered a resource such as employees, computer hardware, computer software, and data.

Authentication – Authentication is the process of ensuring an individual is who they claim to be.

Authorization – Authorization is the process of providing permission to access resources or to perform operations.

Business Continuity – Business Continuity is the ability of an organization to continue its operations and services in the face of a disruptive event.

Business Impact Analysis (BIA) – A Business Impact Analysis is a process that if performed to identify and evaluate the potential impacts of natural and manmade events on business operations.

Cloud Computing – Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Confidential Data – is a generalized term that typically represents **data** classified as Confidential as defined by state or federal statute, regulation or as defined by the Payment Card Industry.

Cryptography - Cryptography is the science of transforming information into a secure form so that it can be transmitted or stored, and unauthorized persons cannot access it.

Custodian – Custodian is the individual or group that is responsible for granting access to data and or network resources.

Data Classification – Data Classification is the process of identifying the levels of protection mechanisms and restrictive access that are required for data based on state or federal statute, regulation and/or criticality and of the data.

Data Validation – Data validation is the process of ensuring that a program operates on clean, correct and useful data.

Hash – A hash is a cryptographic algorithm that can later be decrypted. It is frequently used for comparison purposes to validate the integrity of the data.

Information Systems Council (ISC) – The Information Systems Council is legislatively mandated to provide high level oversight and direction for State of Tennessee information systems and processing.

Input Validation – Input validation is a type of data validation that is applied to data from untrusted sources.

Least Privilege – Least Privilege is a practice where the minimum level of access or privileges required to perform an individual's job duties are granted.

Logic Bomb – A logic bomb is computer code that lies dormant until it is triggered by a specific logical event.

Mobile Device – A mobile device is a computing platform that not meant to be stationary. Examples include but are not limited to laptops, tablets, i-Phones, i-Pads and android devices.

Multifactor Authentication – Multifactor Authentication is using more than one factor to authenticate an individual or resource. Factors include something you know (password), something you have (token or smartcard) and something you are (biometrics such as iris or retinal scans or fingerprints).

Owner – Owner is the individual who is the final authority and decision maker in determining how data and resources are used in State business and what level of access will be granted to them.

Payment Card Industry (PCI) – The Payment Card Industry is comprised of the organizations that transmit, process or store cardholder data. The PCI works with the Payment Card Industry Security Standards Council to develop Payment Card Industry Data Security Standards.

Rootkit – A rootkit is a set of software tools used by an attacker to hide the actions or presence of other types of malicious software.

Salt - A salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase, making the stored data more difficult to crack.

Security Advisory Council – The Security Advisory Council is comprised of the directors in the Office for Information Resources.

Security Event – A security event is an event that adversely impacts the established security behavior of an environment or system

Security Incident - A security incident can be accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of State information and IT assets.

Service Account – A service account is an account that is used by systems, services or applications, not by individuals.

Trojan Horse – A trojan horse (or Trojan) is an executable program advertised as performing one activity, but actually does something else.

Virtual Private Network (**VPN**) – A VPN extends a private network across a public network, such as the Internet. It enables a computer or wireless enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Virus – A computer virus is malicious computer code that reproduces itself on the same computer.

Worm – A computer worm is a malicious program that takes advantage of a vulnerability on one computer and spreads itself to other computers with the same vulnerability.

Deliverable Specification Submission Sheet

TO:

FROM:

Project Name: **Contract Number:**

Project Manager:

The following deliverable:

is now complete. ☐ **It is available for your review**

☐ **Relevant descriptive documents are attached.**

Deliverable contract reference:

Deliverable Frequency:

Deliverable Date(s): Draft date: (if applicable) **Final:**

The deliverable is:

☐ **a document** ☐ **software** ☐ **an event** ☐ **other**

Deliverable Detail

Approval Requirements and/or reference & Deliverable description(s):
• [**Deliverable 1 - description**]

APPROVALS

Prepared By _____
Project Manager

Approved By

_____ Executive Sponsor

_____ Executive Sponsor

_____ Project Sponsor

_____ Project Sponsor

_____ State Project Manager