

Fiscal Review Committee
The Honorable Ron Travis, Chair
The Honorable Todd Gardenhire, Vice-Chair
G-102 Cordell Hull Building
425 Fifth Avenue North
Nashville, TN 37243

Distinguished Members of the Fiscal Review Committee,

The Tennessee Department of Labor & Workforce Development requests an amendment to its contract with Atos IT Solutions & Services, Inc., for the remote hosting and disaster recovery services currently in use with the State's Unemployment Insurance (UI) tax and benefits system. TDLWD requests a one-year extension for these critical services in order to ensure the continuity and safeguarding of UI's claims processing and employer payments. For this reason, the Department will exercise its option for a one-year extension that had been included in the original contract, and will be adding funds necessary to cover these vital services for the next twelve months. The amendment will increase the contract's maximum liability to \$3,960,606.51, the amount agreed upon when the contract was initially presented to the Committee.

The amendment process also provides the opportunity to update the contract's terms to include the State's latest and most up-to-date security language. Therefore the amendment is also designed to improve existing language related to confidential information and data security by adding the most recent requirements approved by the State's Office of Strategic Technology Solutions and the Central Procurement Office.

Sincerely,



Andy Summar, Assistant Commissioner
Finance, Fiscal, & Facilities

Supplemental Documentation Required for
Fiscal Review Committee

*Contact Name:	William Kemmer william.kemmer@tn.gov	*Contact Phone:	615-313-4714		
*Presenter's name(s):	William Kemmer william.kemmer@tn.gov				
Edison Contract Number: <i>(if applicable)</i>	56931	RFS Number: <i>(if applicable)</i>	33701-70617		
*Original or Proposed Contract Begin Date:	11/11/17	*Current or Proposed End Date:	11/11/20		
Current Request Amendment Number: <i>(if applicable)</i>	1				
Proposed Amendment Effective Date: <i>(if applicable)</i>	11/11/19				
*Department Submitting:	Labor & Workforce Development				
*Division:	Information Technology				
*Date Submitted:	8/28/2019				
*Submitted Within Sixty (60) days:	Yes				
<i>If not, explain:</i>	N/A				
*Contract Vendor Name:	Atos IT Solutions & Services, Inc.				
*Current or Proposed Maximum Liability:	\$3,960,606.51				
*Estimated Total Spend for Commodities:	N/A				
*Current or Proposed Contract Allocation by Fiscal Year: (as Shown on Most Current Fully Executed Contract Summary Sheet)					
FY: 20	FY: 21	FY:	FY:	FY	FY
\$1,137,927.55	\$701,140.16				
*Current Total Expenditures by Fiscal Year of Contract: (attach backup documentation from Edison)					
FY: 20	FY:	FY:	FY:	FY	FY
\$436,787.40	\$	\$	\$	\$	\$
IF Contract Allocation has been greater than Contract Expenditures, please give the reasons and explain where surplus funds were spent:			N/A		
IF surplus funds have been carried forward, please give the reasons and provide the authority for the carry forward provision:			N/A		
IF Contract Expenditures exceeded Contract Allocation, please give the reasons and explain how funding was acquired to pay the overage:			N/A		

Supplemental Documentation Required for
Fiscal Review Committee

*Contract Funding Source/Amount:			
State:		Federal:	100%
<i>Interdepartmental:</i>		<i>Other:</i>	
If “ <i>other</i> ” please define:			
If “ <i>interdepartmental</i> ” please define:			
Dates of All Previous Amendments or Revisions: <i>(if applicable)</i>		Brief Description of Actions in Previous Amendments or Revisions: <i>(if applicable)</i>	
Method of Original Award: <i>(if applicable)</i>		Sole-Source Procurement	
*What were the projected costs of the service for the entire term of the contract prior to contract award? How was this cost determined?		The award was originally a non-competitive contract, pricing was determined based on vendor quote.	
*List number of other potential vendors who could provide this good or service; efforts to identify other competitive procurement alternatives; and the reason(s) a sole-source contract is in the best interest of the State.		No other U.S. vendor is authorized to provide remote hosting and disaster recovery services for the [REDACTED] operating environment currently in use by the Department.	



STS Pre-Approval Endorsement Request E-Mail Transmittal

TO : STS Contracts
Department of Finance & Administration
E-mail : it.abc@tn.gov

FROM : William Kemmer
E-mail : william.kemmer@tn.gov

DATE : 04/25/2019 **Received Wednesday July 3, 2019**

RE : Request for STS Pre-Approval Endorsement

Applicable RFS # 33701-40919

State Security Confidential Information Applicability

Under Tenn. Code Ann. §10-7-504(i) vendor identity or a description of the goods or services provided by the vendor shall be confidential.

- Applicable
 Not Applicable

Additional language is attached and endorsement is contingent upon inclusion of this additional language:

- Applicable
 Not Applicable

STS Endorsement Signature & Date:

Chief Information Officer

NOTE: Proposed contract/grant support is applicable to the subject IT service technical merit.

Strategic Technology Solutions (STS) pre-approval endorsement is required pursuant to procurement regulations pertaining to contracts with information technology as a component of the scope of service. This request seeks to ensure that STS is aware of and has an opportunity to review the procurement detailed below and in the attached document(s). This requirement applies to any procurement method regardless of dollar amount.

Please indicate STS endorsement of the described procurement (with the appropriate signature above), and return this document via e-mail at your earliest convenience.

Contracting Agency

Department of Labor & Workforce Development

Applicable RFS # 33701-40919	
Agency Contact (name, phone, e-mail)	William Kemmer 615-313-4714 william.kemmer@tn.gov
<p>Attachments Supporting Request (mark all applicable)</p> <p>Note: The complete draft procurement document and the applicable documents listed below must accompany this request when submitted to STS. Special Contract Requests and Amendment Requests without Agency Head signature are acceptable. STS is aware that these documents will not have CPO signature when submitted with this request.</p> <p><input type="checkbox"/> Solicitation Document</p> <p><input type="checkbox"/> Special Contract Request</p> <p><input checked="" type="checkbox"/> Amendment Request</p> <p><input checked="" type="checkbox"/> Proposed Contract/Grant or Amendment</p> <p><input checked="" type="checkbox"/> Original Contract/Grant and Previous Amendments (if any)</p>	
<p>Information Systems Plan (ISP) Project Applicability</p> <p>To avoid delay of STS pre-approval, the applicability of an ISP project to the procurement must be confirmed with agency IT staff prior to submitting this request to STS. If necessary, agency IT staff should contact STS Planning with questions concerning the need for an ISP project.</p> <p>IT Director/Staff Name Confirming (required): Anthony Starnes</p> <p><input type="checkbox"/> Applicable – Approved ISP Project#</p> <p><input checked="" type="checkbox"/> Not Applicable</p>	
<p>Subject Information Technology Service Description</p> <p>Provide a brief summary of the information technology services involved. Clearly identify included technologies such as system development/maintenance, security, networking, etc. As applicable, identify the contract or solicitation sections related to the IT services.</p> <p>TDLWD seeks continued use of managed mainframe hosting, disaster recovery, and technical support services through Atos IT Solutions & Services. Atos is the sole provider of remote hosting services for the ██████████ operating system currently used in the processing of the State's unemployment insurance claims.</p>	

Attachment: STS Endorsement Conditions

This STS endorsement is contingent upon modification of the procurement documents as described below.

Requirement: STS endorses with the understanding that a. b. and d. from the standard template language below be added to the contract amendment. Please note that Section d (1) contains Recovery options which should be defined based on the agency's business requirements and not be in conflict with Appendix A (1) b) Disaster Recovery.

Recommendation: The current FA template instructs the agency to include Section c. as listed below if the contractor is hosting any state data, even if not confidential.

#. The following is inserted in the contract as Section e.13.

E.13. Contractor Hosted Services Confidential Data, Audit, and Other Requirements
a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

- (1) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.
- (2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.
- (3) The Contractor shall maintain a Security Management Certification from the Federal Risk and Authorization Management Program ("FedRAMP"). A "Security Management Certification" shall mean written confirmation from FedRAMP that FedRAMP has assessed the Contractor's information technology Infrastructure, using a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, and has certified that the Contractor meets FedRAMP standards. Information technology "Infrastructure" shall mean the Contractor's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services. The Contractor shall provide proof of current certification annually and upon State request.

Contractor shall meet all applicable requirements of the most current version of Internal Revenue Service Publication 1075.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

- (4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

Attachment: STS Endorsement Conditions

This STS endorsement is contingent upon modification of the procurement documents as described below.

- (5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State.
 - (6) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.
- b. Minimum Requirements
- (1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: <https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html>.
 - (2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
 - (3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.
- c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

Attachment: STS Endorsement Conditions

This STS endorsement is contingent upon modification of the procurement documents as described below.

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

- d. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:
- (1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:
 - i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: **[NUMBER OF HOURS/MINUTES]**
 - ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: **[NUMBER OF HOURS/MINUTES]**
 - (2) The Contractor **and the Subcontractor(s)** shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recover Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

Attachment: STS Endorsement Recommendations

Recommendation: The agency should replace the original contract PII language (E.7.) with the current FA model language below.

#. Section E.7. Personally Identifiable Information is deleted in its entirety and replaced with the following.

E.7. 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 or ensure 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.

Recommendation: The agency should consult with the CPO regarding the language proposed for Attachment 5.

1. The current FA model contains language specifying requirements for handling FTI data. This language appears to be very similar to the language the agency proposed. STS recommends that the agency use the model language unless CPO allows use of the proposed language instead.

Attachment: STS Endorsement Recommendations

2. Both versions of the FTI language include a statement “Include any additional safeguards that may be appropriate.” If the agency does not intend to define additional safeguards, it should seek CPO permission to delete this statement.

**CONTRACT**

(fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)

Begin Date 11/11/2017	End Date 11/10/2019	Agency Tracking # 33701-70617	Edison Record ID 56931		
Contractor Legal Entity Name Atos IT Service & Solutions, Inc.			Edison Vendor ID 595		
Goods or Services Caption (one line only) Managed mainframe hosting, disaster recovery, and technical support services.					
Contractor <input checked="" type="checkbox"/> Contractor		CFDA #			
Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
18		\$831,976.00			\$831,976.00
19		\$1,289,562.80			\$1,289,562.80
20		\$436,787.40			\$436,787.40
TOTAL:		\$2,558,326.20			\$2,558,326.20
Contractor Ownership Characteristics:					
<input type="checkbox"/> Minority Business Enterprise (MBE):					
<input type="checkbox"/> African American <input type="checkbox"/> Asian American <input type="checkbox"/> Hispanic American <input type="checkbox"/> Native American					
<input type="checkbox"/> Woman Business Enterprise (WBE)					
<input type="checkbox"/> Tennessee Service Disabled Veteran Enterprise (SDVBE)					
<input type="checkbox"/> Disabled Owned Business (DSBE)					
<input type="checkbox"/> Tennessee Small Business Enterprise (SBE): \$10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees.					
<input type="checkbox"/> Government <input checked="" type="checkbox"/> Non-Minority/Disadvantaged <input type="checkbox"/> Other:					
Selection Method & Process Summary (mark the correct response to confirm the associated summary)					
<input type="checkbox"/> Competitive Selection					
<input checked="" type="checkbox"/> Other Non-competitive sole source procurement					
Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.					
<i>M.L. Butler / KW</i>					
Speed Chart (optional)			Account Code (optional)		

**CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT
AND
ATOS IT SOLUTIONS AND SERVICES, INC.**

This Contract, by and between the State of Tennessee, Department of Labor and Workforce Development, hereinafter referred to as the "State" and Atos IT Solutions and Services, Inc., hereinafter referred to as the "Contractor," is for the provision of providing Remote Hosting, Disaster Recovery and other Support services, as further defined in the "SCOPE OF SERVICES."

The Contractor is a For-Profit Corporation
Contractor Place of Incorporation or Organization: Delaware
Contractor Edison Registration ID # 595

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. The purpose of this Contract is for the Contractor to provide the State with Remote Hosting Services, Disaster Recovery Services, Production Control Services, ██████████ Operations Support Services, and ██████████ Remote Technical Support Services in connection with the State's ██████████ environment and ██████████ Computing Facility, including its related communications network, as defined in the Statement of Work attached to this Contract as Appendix A (the "SOW") and incorporated by reference herein (collectively, the "Services").
- A.3. Correction of Deficiencies. Any corrections or 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. Contractor shall maintain normal support for State between the hours of 8:00 a.m. through 5:00 p.m. Monday through Friday, Central Standard Time and all other hours Contractor regularly provides support to customers. Contractor shall respond to State within twenty-four (24) hours, or the next business day should notification occur on a weekend or holiday, of any deficiency identified by State and shall bring to bear all necessary resources to correct any deficiency in the most expeditious manner available.
- A.4. Additional Work. The State may request, at its sole discretion, additional work involving the enhancement or modification of a deliverable under the Contract Scope of Services, provided that this Contract is amended to require such work.
- A.5. Warranty. Contractor represents and warrants that the term of the warranty ("Warranty Period") shall be the greater of: (a) one (1) month after the provision and acceptance by the State of goods or services provided by Contractor; or (b) any other warranty generally offered by Contractor, its suppliers, or manufacturers to customers of its goods or services. During the Warranty Period, 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 the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Contract.
- 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, and in conformity with standards generally accepted in Contractor's industry.
- A.6. Inspection and Acceptance. The State shall have the right to inspect all goods or services provided by the Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify the 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. CONTRACT PERIOD:

- B.1. This Contract shall be effective for the period beginning 11/11/2017, and ending 11/10/2019. This Contractor hereby acknowledges and affirms that the State shall have no obligation for services rendered by the Contractor which were not performed within this specified contract period.
- B.2. Term Extension. The State reserves the right to extend this Contract for an additional period or periods of time representing increments of no more than one year and a total contract term of no more than three (3) years, provided that such an extension of the contract term is effected prior to the current contract expiration date by means of a contract amendment. If a term extension necessitates additional funding beyond that which was included in the original Contract, an increase of the State's maximum liability will also be effected through contract amendment, and shall be based upon payment rates provided in the original Contract.

C. PAYMENT TERMS AND CONDITIONS:

- C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed two million five hundred fifty-eight thousand three hundred twenty-six dollars and twenty cents (\$2,558,326.20). The payment rates in section C.3 shall constitute the entire compensation due the Contractor for all service and Contractor obligations hereunder regardless of difficulty, materials or equipment required. The payment rates include, but are not limited to, all applicable taxes, fees, overheads, and all other direct and indirect costs incurred or to be incurred by the Contractor.

The Contractor is not entitled to be paid the maximum liability for any period under the Contract or any extensions of the Contract for work not requested by the State. The maximum liability represents available funds for payment to the Contractor and does not guarantee payment of any such funds to the Contractor under this Contract unless the State requests work and the Contractor performs said work. In which case, the Contractor shall be paid in accordance with the payment rates detailed in Section C.3. 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.

- C.2. Compensation Firm. The payment rates and the maximum liability of the State under this Contract are firm for the duration of the Contract and are subject to escalation provisions as detailed in Section C.10 of this Contract.
- C.3. Payment Methodology. The Contractor shall be compensated based on the payment rates herein for units of service authorized by the State in a total amount not to exceed the Contract Maximum Liability established in section C.1.
 - a. The Contractor's compensation shall be contingent upon the satisfactory completion of units, milestones, or increments of service defined in section A.
 - b. The Contractor shall be compensated for said units, milestones, or increments of service based upon the following payment rates:

<u>SERVICE DESCRIPTION</u>	<u>AMOUNT</u> (per compensable increment)
Managed Hosting Services Fee Effective 11/11/2017	\$ 86,635 per Month*
Including Disaster Recovery Services for [REDACTED] and Remote VPN Services for up to twenty-five (25) named employees (according to the records that document the number of state employees who log on at least once during the calendar month for Remote VPN Services).	

Production Control Services Fee Effective 11/11/2017	\$3,702 per Month
Operations Support Services Fee Effective 11/11/2017.	\$7,451 per Month
Remote Technical Support Services Fee Effective 11/11/2017 - Up to 1,000 Hours per Year	\$6,209 per Month
Hourly Rate for Remote Technical Support Services in Excess of Contracted 1,000 Hours per Year - Optional	\$104 per Hour

- C.4. Travel Compensation. The Contractor shall not be compensated or reimbursed for travel, meals, or lodging.
- C.5. Invoice Requirements. The Contractor shall invoice the State only for completed increments of service and for the amount stipulated in Section C.3, above, and present said invoices no more often than monthly, with all necessary supporting documentation, to:

Tennessee Department of Labor &
Workforce Development
220 French Landing Drive, 4A
Nashville, TN 37243-1002

- a. Each invoice shall clearly and accurately detail all of the following required 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: Labor and Workforce Development & Employment Security
 - (5) Customer Account Number (assigned by the Contractor to the above-referenced Customer)
 - (6) Contractor Name
 - (7) Contractor Tennessee Edison Registration ID Number Referenced in Preamble of this Contract
 - (8) Contractor Contact for Invoice Questions (name, phone, and/or fax)
 - (9) Contractor Remittance Address
 - (10) Description of Delivered Service
 - (11) Complete Itemization of Charges, which shall detail the following:
 - i. Service or Milestone Description (including name & title as applicable) of each service invoiced
 - ii. Number of Completed Units, Increments, Hours, or Days as applicable, of each service invoiced
 - iii. Applicable Payment Rate (as stipulated in Section C.3.) of each service invoiced
 - iv. Amount Due by Service
 - v. Total Amount Due for the invoice period
- b. The Contractor understands and agrees that an invoice under this Contract shall:
- (1) include only charges for service described in Contract Section A and in accordance with payment terms and conditions set forth in Contract Section C;
 - (2) only be submitted for completed service and shall not include any charge for future work;
 - (3) not include sales tax or shipping charges; and

- (4) initiate the timeframe for payment (and any discounts) only when the State is in receipt of the invoice, and the invoice 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 matter in relation thereto. A payment by the State shall not be construed as acceptance of any part of the work or service 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 theretofore made which are determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, not to constitute proper remuneration for compensable services.
- 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, which 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 documentation properly completed.
- a. The Contractor shall complete, sign, and present to the State an "Authorization Agreement for Automatic Deposit (ACH Credits) Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once said form is received by the State, all payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee shall be made by Automated Clearing House (ACH).
- b. The Contractor shall complete, sign, and present to the State a "Substitute W-9 Form" provided by the State. The taxpayer identification number detailed by said form must agree with the Contractor's Federal Employer Identification Number or Tennessee Edison Registration ID referenced in this Contract.
- C.10. Fee Increases: Effective on November 11, 2018, all fees in Section C.3. under this Contract will be increased by Atos by 5%. Beginning November 11, 2019, for the third option year, the monthly fees will be increased by an amount not greater than the percentage change in the Consumer Price Index for Urban Wage Earners CPI-W as published by the Bureau of Labor Statistics, U.S. Department of Labor over the previous year.

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:

William Kemmer, Contract Specialist
Labor & Workforce Development
220 French Landing Drive, Nashville, TN 37423
william.kemmer@tn.gov
Telephone # 615-313-4714

The Contractor:

James Ulrey, Director NAO-BDS
Atos IT Solutions and Services, Inc.
13430 N. Black Canyon Hwy, #280, Phoenix, AZ 85029
Telephone # 602-862-5001

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.
- 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 ninety (90) 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 of 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 Reference A, 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 three (3) 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 venturers, 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 Liability. Each Party shall have no liability except as specifically provided in this Contract. In no event will a Party be liable to the other party or any other party for any indirect losses in the nature of lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any other 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. Each Party'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 actual charges paid by the State to the Contractor for the period that such Services caused the actual damage. This limitation of liability is cumulative and not per incident. PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.
- D.18. 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.19. 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.20. 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.21. 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.22. 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, disqualified, or presently fall under any of the prohibitions of sections a-d.

- D.23. 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.24. State and Federal Compliance. The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.
- D.25. 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.26. 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.27. 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.28. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.29. 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), which includes Appendices A & B and Attachments 1-4;
 - 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.
- D.30. Iran Divestment Act. The requirements of Tenn. Code Ann. § 12-12-101 et.seq., addressing contracting with persons as defined at T.C.A. §12-12-103(5) that engage in investment activities in Iran, shall be a material provision of this Contract. The Contractor certifies, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.
- D.31. Insurance. Contractor shall maintain insurance coverage as specified in this Section. The State reserves the right to amend or require additional insurance coverage, coverage amounts, and endorsements required under this Contract. Contractor's failure to maintain or submit evidence of insurance coverage, as required, is a material breach of this Contract. If Contractor loses insurance coverage, fails to renew coverage, or for any reason becomes uninsured during the Term, Contractor shall immediately notify the State. All insurance companies providing coverage must be: (a) acceptable to the State; (b) authorized by the Tennessee Department of Commerce and Insurance ("TDCI"); and (c) rated A- / VII or better by A.M. Best. All coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State. Contractor agrees to name the State as an additional insured on any insurance policy with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) insurance. All policies must contain an endorsement for a waiver of subrogation in favor of the State. Any deductible over fifty thousand dollars (\$50,000) must be approved by the State. The deductible and any premiums are the Contractor's sole responsibility. 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.

To achieve the required coverage amounts, a combination of an otherwise deficient specific policy and an umbrella policy with an aggregate meeting or exceeding the required coverage amounts is acceptable. For example: If the required policy limit under this Contract is for two million dollars (\$2,000,000) in coverage, acceptable coverage would include a specific policy covering one million dollars (\$1,000,000) combined with an umbrella policy for an additional one million dollars (\$1,000,000). If the deficient underlying policy is for a coverage area without aggregate limits (generally Automobile Liability and Employers' Liability Accident), Contractor shall provide a copy of the umbrella insurance policy documents to ensure that no aggregate limit applies to the umbrella policy for that coverage area.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified in this Section. The COI must be on a form approved by the TDCI (standard ACORD form preferred). The COI must list each insurer's National Association of Insurance

Commissioners (NAIC) number and be signed by an authorized representative of the insurer. The COI must list the State of Tennessee – CPO Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 as the certificate holder. Contractor shall provide the COI ten (10) business days prior to the Effective Date and again thirty (30) calendar days before renewal or replacement of coverage. Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that subcontractors are included under the Contractor's policy. At any time, the State may require Contractor to provide a valid COI. The parties agree that failure to provide evidence of insurance coverage as required is a material breach of this Contract. If Contractor self-insures, then a COI will not be required to prove coverage. Instead Contractor shall provide a certificate of self-insurance or a letter, on Contractor's letterhead, detailing its coverage, policy amounts, and proof of funds to reasonably cover such expenses.

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.

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).

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 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 employs 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. Automobile Liability Insurance

- 1) The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).
- 2) The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars (\$1,000,000) per occurrence or combined single limit.

D.32. Major Procurement Contract Sales and Use Tax. Pursuant to Tenn. Code Ann. § 4-39-102 and to the extent applicable, the Contractor and the Contractor's subcontractors shall remit sales and use taxes on the sales of goods or services that are made by the Contractor or the Contractor's subcontractors and that are subject to tax.

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. Intellectual Property Indemnity. 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, 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.3. Software License Warranty. Contractor grants a license to the State to use all software provided under this Contract in the course of the State's business and purposes.

E.4. Software Support and Maintenance Warranty. Contractor shall provide to the State all software upgrades, modifications, bug fixes, or other improvements in its software that it makes generally available to its customers.

E.5. 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.6. 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.7. 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.
- E.8. There are no express or implied warranties, including the implied warranties of merchantability and fitness for a particular purpose not specified herein respecting this agreement or the services, products, materials and documentation provided. Contractor does not warrant that the use of the software products will be uninterrupted or that the software products are error-free.
- E.9. Any Reseller or third party receiving the State's orders for service hereunder or providing any service for Contractor hereunder is not a partner, agent, employee or franchisee of Contractor and has no authority to bind Contractor or to assume or create any obligations express or implied on behalf of Contractor or in Contractor's name. Contractor and the State are not partners, agents, employees or franchisees of each other.
- E.10. Contractor Confidential Information and Contractor Software. Contractor warrants to the State that it has the right to disclose all confidential information it discloses to the State under the obligations of confidentiality as set forth herein. The State agrees to retain in confidence and not disclose to others any information, whether or not in written form, of Contractor, including, but not limited to, trade secrets, marketing materials, data compilations, business plans, user data and technical information, which is designated as confidential by Contractor at the time it is

disclosed to the State or which the State otherwise knows is confidential ("Contractor Confidential Information"). The State agrees that all Contractor Confidential Information will remain the exclusive property of Contractor and that during the term of this Contract and for three (3) years from its expiration or termination: (i) it will maintain, and will use prudent methods to cause its employees and agents to maintain, the confidentiality and secrecy of the Contractor Confidential Information; (ii) it will use prudent methods to see that it and its employees and agents do not copy, publish, disclose to others or use (other than pursuant to the terms hereof) the Contractor Confidential Information; (iii) it will return or destroy all copies of Contractor Confidential Information for any purpose other than as permitted in this Contract. It is further agreed that the terms and conditions of this Contract are confidential, provided that the existence of this Contract and descriptions of the Services hereunder may be disclosed in press release and other marketing collateral.

Notwithstanding the foregoing, Contractor Confidential Information will not include any information to the extent it (i) is or becomes a part of the public domain through no act or omission on the part of the State; (ii) is disclosed to third parties by the Contractor without restriction on such third parties; (iii) is in the State's possession, without actual or constructive knowledge of an obligation of confidentiality with respect thereto, at or prior to the time of disclosure under this Contract; (iv) is disclosed to the State by a third party having no obligation of confidentiality with respect thereto; (v) is independently developed by the State without reference to or use of the Contractor's Confidential Information; or (vi) is released from confidential treatment by written consent of the Contractor. The State may disclose the Contractor's Confidential Information to the extent required to be disclosed by a court or governmental agency pursuant to a statute, regulation or valid order; provided that the State first notifies the Contractor and gives the Contractor the opportunity to seek a protective order or to contest such required disclosure.

The State shall have no obligation to treat as confidential any information that was in the State's possession without binder of secrecy prior to receipt from the Contractor, is independently developed by the State or is or becomes public knowledge independent of any act by the State.

All software and related documentation (a) owned or licensed by Contractor prior to the Effective Date which is necessary to or used in connection with the Services or (b) which Bull Services acquires ownership of or license rights in after the Effective Date and which are necessary to or used in connection with the Services (collectively the "Contractor Software" or "Bull Software") shall be and shall remain the exclusive property of Bull, and the State shall have no rights or interests in the Bull Software except as may be expressly provided in this Contract.

As part of the Services, Contractor shall:

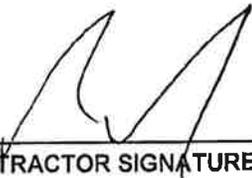
- (a) use the Bull Software as identified in Appendix A as being supplied by Bull and such other system software as the State and Bull may agree from time to time (collectively, the "Bull Software"); and
- (b) make available the Bull Software to the State for its use on the Bull computer systems as identified in Appendix A, Section (1) xvi. (collectively the "Bull System"), as they may be modified by an approved RFC, provided that such right to use by the State shall be limited to such use as is necessary to make effective use of the Services. The State further agrees that Bull Software is confidential information, which shall be treated in accordance with this Section E.10 of this Contract.

- E.11 Contractor is not liable for any loss, destruction or damage to the State's application programs and data files unless due solely to the fault of Contractor and then only to the extent of restoring the lost, destroyed or damaged programs and data files, provided that such restoration can be reasonably performed by Contractor. The State shall furnish Contractor with all information necessary for such restoration.
- E.12. For all claims arising under this Agreement that are not covered by a service credit as set forth in Appendix A, the State's exclusive remedy and Contractor's entire liability in contract, tort, negligence or otherwise arising out of or in any way connected with Services hereunder is the payment by the Contractor of actual damages not to exceed the actual charges paid by the

State to Contractor for the period that such Services caused the actual damage. For any claims arising under this Agreement that are covered by a service credit set forth in Appendix A, Section 9, such service credit shall constitute the State's sole and exclusive remedy and Contractor's entire liability.

IN WITNESS WHEREOF,

ATOS IT SOLUTIONS & SERVICES, INC.:



CONTRACTOR SIGNATURE

9 Nov 2017

DATE

STEPHEN SHIBEL SVP Big Data / Cyber

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

DEPARTMENT OF LABOR & WORKFORCE DEVELOPMENT:

Burns P. Phillips III

BURNS PHILLIPS III, COMMISSIONER

11/9/17

DATE

Appendix A

Statement of Work (“SOW”)

The Services to be supplied by Atos consist of the following:

- (1) Managed Hosting Services
 - a. Remote hosting
 - b. Disaster recovery
- (2) Production Control Services
- (3) ██████████ Operations Support Services
- (4) ██████████ Remote Technical Support Services
- (5) Hosting Facility Security Requirements

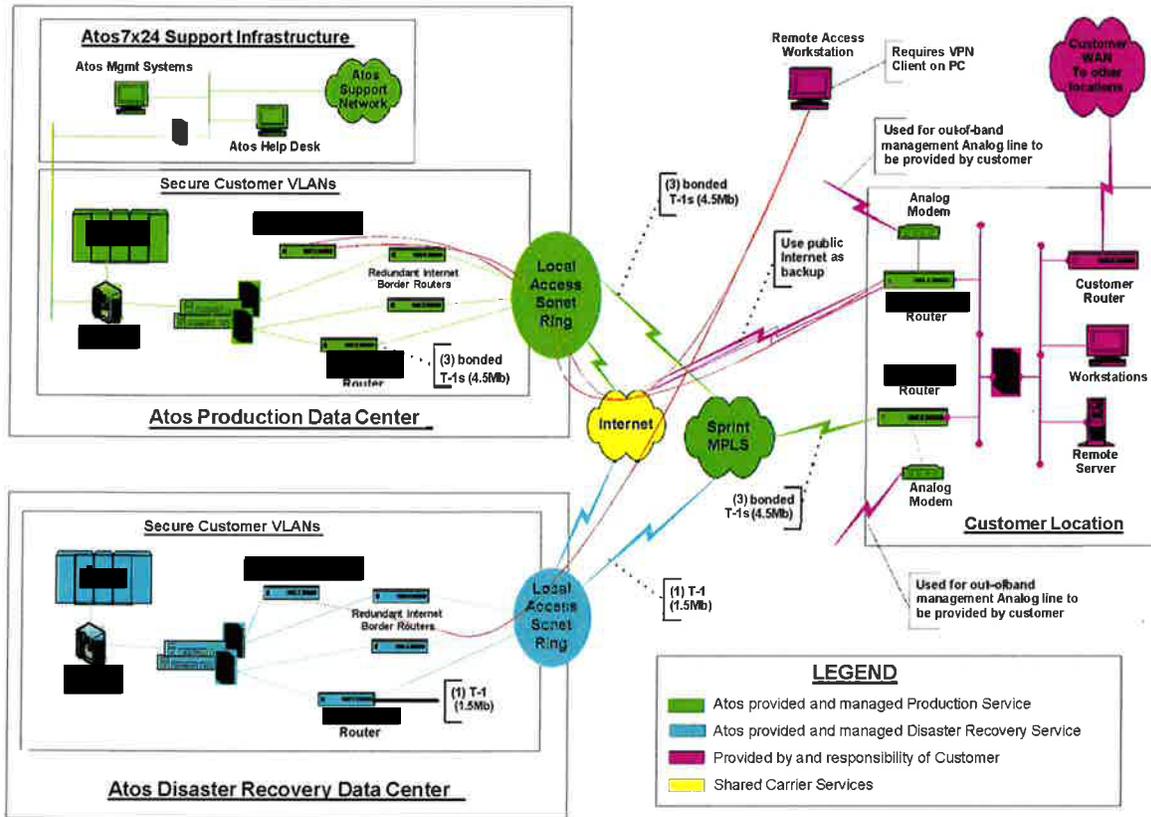
The following apply to all Services:

- (6) Limitations
- (7) State Responsibilities
- (8) Joint Responsibilities
- (9) Service Level Agreement
- (10) Other

(1) Managed Hosting Services

- a) Remote Hosting. For remote hosting Atos will provide:
 - i. A communications environment within the Atos Data Center that separates the State’s communications infrastructure from any other Atos customer. Atos and the State’s responsibilities for the communications environment are depicted in the following diagram.

Atos Managed Service for State of Tennessee



- ii. Network monitoring and repair of its network services 7 x 24 through its automated Atos Network Management Center. Atos will supply to the State general network availability metrics for segments of the network under the direct responsibility of Atos.
- iii. Software that is necessary to facilitate the Services provided by Atos, where such software is part of the Atos Provided Software set forth in Attachment 4 attached to this SOW.
- iv. Network infrastructure to segregate the State from other Atos customers while allowing limited access to the State [REDACTED] systems at the Atos Data Centers.
- v. Internet access at the Atos Data Centers allowing remote client VPN access to the State systems.
- vi. An Atos 7x24 fully managed [REDACTED] router at the Atos Production Data Center. This router is used to terminate three (3) T-1 MPLS ports provided by Atos. The router is configured so that the three (3) T-1s are bonded to provide a 4.5Mb connection between the remote State location and the Atos Production Data Center.
- vii. A [REDACTED] VPN device at the Atos Production Data Center allowing up to twenty-five (25) named remote users secure access via

the Internet to the State's applications on a monthly basis. This [REDACTED] device is also used to terminate the backup secure VPN tunnel via the public Internet. This tunnel provides connectivity between the State location and the Atos Production Data Center, should the MPLS service be unavailable.

- viii. An Atos 7x24 fully managed [REDACTED] router at the State location. This router is used to terminate three (3) T-1 MPLS ports provided by Atos. The router is configured so that the three (3) T-1s are bonded to provide a 4.5Mb connection between the remote State location and the Atos Production Data Center. The router has an Atos provided modem attached to the console port on the router to be used for out-of-band management. The State will provide a dedicated analog line to be attached to the Atos provided router.
- ix. An Atos 7x24 fully managed [REDACTED] router at the State location. This router is used to terminate a secure VPN tunnel that provides backup connectivity via the public Internet should the dedicated MPLS connection be unavailable. The Internet access at the State's location is provided by the State. The router has an Atos provided modem attached to the console port on the router to be used for out-of-band management. The State provides a dedicated analog line that is attached to the Atos provided router.
- x. An Atos 7x24 fully managed Cisco 1841 router at the Atos Disaster Recovery Data Center. This router is used to terminate a T-1 MPLS port provided by Atos. The router is configured to provide a T-1 connection between the remote State location and the Atos Disaster Recovery Data Center.
- xi. Atos will provide a VPN tunnel from the Atos Disaster Recovery Data Center to the State location for access to the ICON system.
- xii. A [REDACTED] VPN device at the Atos Disaster Recovery Data Center allowing up to twenty-five (25) named remote users secure access via the Internet to the State's applications on a monthly basis.
- xiii. Atos will assign public Internet IP addresses to the devices managed by Atos in the Atos Data Centers. The State will provide Atos a public Internet routeable IP address for any device managed by Atos at a State location.
- xiv. Atos will provide redundant core switches and will use VLANs and firewalls to logically segregate the State's network environment from other Atos customers at the Atos Data Centers.
- xv. Atos will supply the Atos Operating System Software required to provide the Remote Hosting Services.
- xvi. Atos will provide the following configuration (the "Atos System"):

Qty	Description
1	Access to a dedicated [REDACTED] partition on a shared [REDACTED]
400GB	Disk space dedicated for the State's volsets Media Server – Owned by the State
1	DataBase Server Processor (DBSP) - Owned by the State

- xvii. Atos will provide off-site tape storage and rotation.
 - xviii. Atos will provide a Help Desk function which will be accessible to designated personnel of the State twenty-four (24) hours a day, three hundred and sixty-five (365) days a year. Once calls are qualified, they shall be routed to the appropriate support personnel. Notification is provided to the State regarding progress on resolution, and final outcome.
 - xix. Atos will provide an individual, acceptable to the State, to act as account manager. The account manager will be the primary contact between Atos and the State for questions, problem identification and resolution, and billing issues.
 - xx. Atos will provide the software described in Attachment 4 (the "Atos Provided Software"). The extent to which the Atos Provided Software will be supported by Atos as part of this Agreement shall be Full Support, Limited Support or No Support. The level of software support for the Atos Provided Software in effect as of the Effective Date of this Agreement is set forth in Attachment 4. Atos shall have the right to change the level of software support for the applicable Atos Provided Software effective upon written notice to the State. For purposes of this SOW, the following definitions shall apply:
 - a. Full Support – Atos shall use reasonable efforts to provide software that conforms to its published specifications through problem research, engineering support through the opening and processing of System Technical Action Requests ("STARs"), the development and application of temporary fixes and/or emergency bypasses as well as searching and making available the results of any known problem files and for those items of Atos Provided Software that are designated as owned by a third party, then all of the foregoing is subject to the extent any support is available from such third party.
 - b. Limited Support – Atos shall use reasonable efforts to provide software that conforms to its published specifications through the application of previously developed temporary fixes and/or emergency bypasses and making available the results of known problem files, if any.
 - c. No Support – No support is provided at all.
- b) Disaster Recovery. For disaster recovery Atos will provide:

- i. If the Atos System is expected to be unavailable for use for more than forty eight (48) continuous hours for reasons not caused by nor under the control of the State, then if the State affirmatively certifies in writing to Atos that a disaster situation exists for State, then Atos shall utilize a disaster recovery system with an initial configuration equivalent to that set forth in Appendix A, Section (1) a) xvi. (the "Disaster Recovery System Configuration") located at a designated Atos Disaster Recovery Data Center to provide Disaster Recovery Services to the State, unless the State decides not to use such Services. Atos may make changes to the Disaster Recovery System Configuration (additions, replacements, modifications). Such equipment changes by Atos will provide equal or greater functionality. Atos shall notify the State of all changes to the Disaster Recovery System Configuration and shall provide the State with a reasonable amount of Testing Use time if any such change would significantly affect the State's backup recovery procedures and operation.
- ii. The State acknowledges and agrees that while the Atos Disaster Recovery Data Center shall not be in the same facility as the Atos Remote Hosting Data Center, the Atos Disaster Recovery Data Center may be in the same geographic region as the Atos Remote Hosting Data Center.
- iii. The State agrees to cooperate with Atos in the event of a disaster, to assist in the relocation of the State's workload processing to the Disaster Recovery Facility and in the relocation back to the Atos Remote Hosting Data Center.
- iv. In order to familiarize the State with the operation of its programs on the Disaster Recovery System configuration and to facilitate the State's development and testing of backup recovery procedures, Atos shall make available to the State at no additional charge up to 96 continuous hours of Testing Use time during each 12 month period of this Contract commencing on the Effective Date. In the event of an actual Disaster declared by the State, if and to the extent the State needs to re-locate any equipment, such as a printer, to the Atos's Disaster Recovery Facility, Atos will cooperate with the State and define a mutually acceptable Request for Change to set forth the terms, conditions and charges, if any, associated with the set up, installation and operation of such equipment, which equipment would be relocated at the State's sole cost and expense.
- v. This Agreement does not provide nor is it intended to provide to the State a guarantee of immediate access or exclusive or uninterrupted use of the Atos Disaster Recovery facilities. The State acknowledges that Atos offers Disaster Recovery Services to other customers/prospects and that a potential scheduling conflict for Disaster Recovery Use of Atos's Disaster Recovery facility could arise. In the event of such an occurrence, Atos will negotiate with the State and any other involved party to arrange an equitable scheduling of use time.

(2) Production Control Services

- a) Atos will provide [REDACTED] Production Control services. Atos Production Control Services will be provided Monday through Friday during the Prime Shift Central Time. Atos will provide Production Control Services for the State's [REDACTED] production processing consisting of the following tasks:
- i. Manage the automated scheduler and modify daily schedules, as needed.
 - ii. Monitor production jobs using the tools provided by the State as well as Atos provided tools and techniques.
 - iii. Provide the State with a morning report depicting processing results for Production Job processing over the previous 24 hour window.
- b) State Responsibilities. The State is responsible for:
- i. Providing Atos with detailed daily processing schedules depicting job dependencies, job schedules and processing priorities.
 - ii. Maintaining production processing schedules, run dependencies.
 - iii. Providing Atos with documented restart and recovery procedures for all production jobs being processed and monitored by Atos.
 - iv. Providing Atos with contact information for problem resolution of aborted jobs.
 - v. Notifying Atos of schedule and production job processing changes using a Atos and State jointly developed change methodology process.
 - vi. Providing and maintaining any tools that are required for Production Control functions.
 - vii. Providing Atos with reasonable access to the State's key personnel during the term of this Contract.

(3) Computer Operations Services

- a) Atos will provide [REDACTED] Operations Support services. Atos Computer Operations Services will be provided Sunday through Saturday 24 hours per day. Atos will provide [REDACTED] Operations Support Services for the State's [REDACTED] production processing consisting of the following tasks:
- i. Abort notification for Production Jobs that do not complete in a normal manner. Atos will notify the State's designated representative for resolution of aborted job. Notification will be by cell phone, email or office telephone. Resolution of the aborted job will be by the State's designated representative with restarts performed by the State's representative and Atos production control staff.
 - ii. Responding to console messages from State production programs per agreed upon procedures.
 - iii. Responding to requests from State programmers for console and tape questions.

- b) State Responsibilities. The State is responsible for:
- i. Providing Atos with detailed daily processing schedules depicting job dependencies, job schedules and processing priorities.
 - ii. Providing Atos with documented restart and recovery procedures for all production jobs being processed and monitored by Atos.
 - iii. Providing Atos with contact information for problem resolution of aborted jobs.
 - iv. Providing and maintaining any tools that are required for operations support function.
 - v. Providing Atos with reasonable access to the State's key personnel during the term of this Contract.

(4) Remote Technical Support Services

- a) Atos will provide [REDACTED] Remote Technical Support Services. Remote Technical Support Services will be provided Monday through Friday during the Prime Shift Central Time. Atos will provide Remote Technical Support Services for the State's [REDACTED] production processing consisting of the following tasks:
- i. Providing [REDACTED] operating system technical support to Operations, Production Control and the State's programming staff.
 - ii. Maintaining [REDACTED] product configurations (e.g. [REDACTED] excluding the DBSP configuration).
 - iii. Providing the first level support for 3rd party products on the [REDACTED] production system (e.g. Louis).
- b) The State is responsible for:
- i. Providing the proper training for the Atos [REDACTED] technical support employees prior to the turnover of any work from the State.
 - ii. Providing Atos with access to their network and system resources, computer time, and other assistance as required for [REDACTED] System Administration activities.
 - iii. Providing Atos with the State's specific practices and processes for recovering from or addressing issues that may occur during production processing and require Technical Support Services.
 - iv. Provide Atos with the State's specific documentation on file locations, user ID information, and contact names/phone numbers for State individuals that must address application issues.
- c) The Technical Support Services are capped at one thousand (1,000) hours per Contract Year. Excess hours beyond one thousand hours will be billed at the hourly rate stated in Section C.3.b of the Agreement. Excess hours must be pre-approved by the State. Atos does not guarantee the availability of personnel beyond one hundred and sixty (160) hours in any calendar month.

(5) Hosting Facility Security Requirements

1. The contractor shall ensure that all confidential State data is housed only in the United States, including backup.
2. The contractor shall encrypt confidential State data in transit using the current version of Federal Information Processing Standard (FIPS) 140-2 validated encryption technologies.
3. The contractor must comply with the State's Enterprise information Security Policies.
4. The contractor agrees to maintain operating systems at current, manufacturer supported versions.
5. The contractor agrees to allow the State to perform logical and physical audits of the facility and systems.
6. The contractor must annually perform penetration tests and vulnerability assessments against its processing environment.
7. The contractor agrees to let the State perform penetration tests and vulnerability assessments against the contractor's processing environment with prior notice on a mutually agreeable schedule.
8. Upon State request, the contractor shall provide a copy of the State data it holds. The contractor shall provide such data on a media format compatible with the Atos GCOS operating environment.
9. Upon termination of this contract and in consultation with the State, the contractor shall destroy all confidential State data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology (NIST) Special Publication 800-88. The contractor shall provide a written confirmation of destruction to the State.

(6) Limitations

- a. Atos is responsible for only the network infrastructure it supplies.
- b. Atos may at any time change its Internet Service Provider (ISP) as may be necessary for Atos to supply the services in the most appropriate manner and/or to best address the State's then current workload requirements. The State will be given advance written notice of any changes, which would affect its processing. An RFC will be processed if such changes result in increased Managed Hosting Service Fees.
- c. Atos is not responsible or otherwise liable for and makes no representation or warranty in connection with the adequacy of the three (3) T-1 devices.

(7) State Responsibilities

- a. Providing on-site personnel at each State location to assist Atos with the implementation and support of the WAN service and the routers provided by Atos.
- b. The installation of the VPN clients on all State workstations. The State will be responsible for the support of the remote workstations.
- c. Provisioning and associated charges for the analog lines at each of the remote locations.
- d. Providing any internal wiring required at the State facility to install

circuits between the State's site and the Atos Data Center.

- e. Internet Access of remote workstations.
- f. Internet Access at each State location.
- g. Providing the third party software products and maintain vendor support contracts for the software products listed in Attachment 1, which software products shall be considered "State Software", as defined below, and providing the hardware listed in Attachment 2, which hardware products shall be considered "State Hardware", as defined below.
- h. Print processing and output distribution.
- i. The State's application programs, synchronization of program changes, database file contents, database administration and Transaction Processing (TP) administration.
- j. The State's Help Desk taking the first call for end user issues and dispatch unresolved calls to Atos's Customer Support Center.
- k. The State shall designate no more than two individuals as its representatives, at least one of whom shall be available to Atos during Regular Business Hours to coordinate activities hereunder. For the purpose of this Section, "Regular Business Hours" means 8:00 a.m. to 5:00 p.m. Mountain Time, Monday through Friday, excluding all Atos holidays. The State shall also provide Atos a single point of contact for coordination of all technical and operation matters.
- l. Providing reasonable access to the State's key personnel during the term of the Contract.
- m. Obtaining the necessary rights and maintenance for Atos to have access to all third party software products for use in supporting the State's workload.
- n. Providing reasonable facility support, protection, and security for equipment provided by Atos at the State's site, and reasonable access to such equipment all at no cost to Atos.
- o. The State shall be solely responsible for the security, completeness, accuracy, reliability, compatibility and timely delivery of its data, files and programs and all results to be obtained there from. Further, the State shall implement such other reasonable security measures as may be recommended by Atos to provide security for the State's data and files.
- p. The State agrees to take all reasonable and necessary steps to see that each of its users who access the Atos System does so only in accordance with the terms and conditions of this Contract and Atos security requirements and refrains from any activity which may interfere with, disrupt or damage the Services or the Atos System. Only State employees or State subcontractors may use the Services described in Appendix A. The State agrees that it is solely responsible for such

persons and for instructing them in the obligations of the State under this Contract in connection therewith.

- q. The State represents and warrants to Atos, with respect to all software used by the State in connection with this Contract, which is not Atos supplied software and which either operates on or communicates with the Atos System (the "State Software"), that the State, either owns or has the right to (a) use the State Software on the Atos System and (b) permit Atos to use State Software on the Atos System, all for the purposes of this Contract. The State further represents and warrants to Atos, with respect to any hardware that is to be furnished by the State to Atos, including, without limitation, the hardware identified in Attachment 2 to this Appendix A (collectively, the "State Hardware"), that the State either owns or has the right to (a) use the State Hardware and (b) permit Atos to use the State Hardware, all for the purposes of this Contract. It is agreed that Atos has no obligation to supply or maintain any State Software or State Hardware.
- r. The State represents and warrants that no data, files, code or programs owned by the State and furnished by the State to Atos in connection with this Contract shall contain any viruses, code or other programming that is designed to corrupt, damage or otherwise adversely affect computer programs, data, hardware, or Atos Software.
- s. The State grants Atos the right to operate the State Software on the Atos System for all purposes consistent with the furnishing of the related Services.
- t. The State shall comply with any and all security rules and regulations while in Atos facilities.

(8) Joint Responsibilities

- a. Atos and the State will mutually agree to IP addressing to be used within the Data Centers and at the State location.
- b. Atos and the State will work together to resolve any service problems associated with the implementation and operations of the end to end VPN service.
- c. Atos and the State will work together to resolve any remote workstation access problems using the VPN client via the Internet.
- d. Atos and the State will mutually agree to processes and procedures associated with service problems involving the router at the remote location.
- e. Atos and the State will work together to resolve any connectivity issues between the State desktops and the Atos Data Center.

(9) Service Level Agreement

- a. Atos provides a service level agreement (SLA) of 99.0% availability for the Atos System.

If Atos fails to meet the overall System Availability requirement of 99.0% in any calendar month for the Atos System, a service credit shall become due in

an amount equal to one percent (1.0%) of that month's monthly managed hosting service fee for each full percentage point that System Availability is below 99.0%. A "Service Credit" in this amount shall appear on the next month's invoice to the State.

Overall "System Availability" is defined and calculated as follows:

$$\left[\frac{(A - B) - C}{(A - B)} * 100 \right]$$

where:

"A" equals the total available hours;

"B" equals the maintenance time including:

- Preventive Maintenance and other normal scheduled maintenance hours
- Any approved special maintenance hours
- The total period of time between Atos' originally requested time for Emergency Maintenance and the scheduled start time granted by the State

"C" equals the Downtime.

"Downtime" shall be the duration of any period of time during which the Atos System is not providing computing services because of a failure of the VPN (Internet) from the Atos demarcation ("Network Access") to the Atos System, or a failure of the Operating System software, the central processing unit or other critical system hardware, or more than fifty percent (50%) of any one of the following:

- i. Network Access,
- ii. Disk subsystem or
- iii. Central processing unit processing capacity, provided that such period is not Preventive Maintenance (scheduled downtime) nor is it primarily caused by or under the control of the State or by any failure by the State's Internet Services Provider.

If it cannot be determined that Downtime affecting System Availability was caused by or was under the control of either party, then the occurrence will be logged as "under investigation, cause not determined." The occurrence will be documented, but not considered downtime. If there is an occurrence of the same type of failure within the following ninety (90) days, and it is then determined that Atos is the responsible party, the appropriate service credit(s) will be issued for all previous failures of the same type occurring during the previous ninety (90) day period. This service credit will be issued in the same month that the cause of the problem was identified. If the failure is determined to be caused by or under the control of the State, the failure, and all failures of the same type during the preceding ninety (90) day period will be logged as "closed," and the cause of the failure will be specified and recorded. Atos shall continue to maintain complete and comprehensive records of the unclassifiable problems, and report them in accordance with the terms in force.

"Preventive Maintenance" is defined as those activities performed by Atos that are necessary or desirable for the continuous provision of overall System Availability, including but not limited to, those activities that require the temporary cessation of Service. Preventive Maintenance may be planned and performed from time to time by Atos. Contractor agrees to provide the State annually with a preventive maintenance schedule for the next calendar year within thirty (30) days after receiving from the State a fiscal calendar showing closing periods.

"Emergency Maintenance" is defined as any maintenance activities performed by Atos after consulting with the State, upon Atos becoming aware of the likelihood that system degradation may result in an imminent further degradation of service and/or total cessation of service. Emergency Maintenance activities shall be performed prior to or during the occurrence of such a degradation, and shall include such actions that are reasonable and necessary to prevent a further degradation and/or total cessation of service, and to restore service with the least possible impact to end users. Emergency

Maintenance activities are those that cannot reasonably be deferred until the next scheduled maintenance period without incurring an unacceptable risk of a further degradation of service and/or a total cessation of service. Once Atos notifies the State of the need for an Emergency Maintenance period no service credits for System Availability will apply for the period of time between being notified and the time when the Emergency Maintenance period actually begins.

(10) Other

- a. The network and remote printing environment is intended to support the State's [REDACTED] processing requirements as of the Effective Date of this Contract. Any changes in State requirements after the Effective Date shall be considered outside the scope of this Contract.
- b. All equipment furnished by Atos to the State under this Contract, remains the property of Atos and shall be returned to Atos upon termination of this Contract.
- c. Atos may at any time change the Atos System to provide the most efficient operating environment for the State and/or to best match the State's then current workload requirements. The State will be given advance notice of any changes which would affect its processing.
- d. The State acknowledges that Atos shall have the right, during the Term of this Contract, to move the location of the Atos Data Center from where some or all of the Services defined in a SOW are performed (including those Services described in Sections 1 through 4 of this SOW) and where some or all of the Atos provided hardware, Atos Software, State Software and/or State Hardware used to perform such Services are located, to the extent Atos determines, in its sole discretion, that such a move would enable Atos to deliver the Services in a more cost effective or efficient manner. Any such move shall not materially disrupt, inhibit or lessen the Services or quality and level of such Services provided to the State by Atos, provided that (a) the State acknowledges and agrees that there shall be a mutually agreed upon, coordinated outage of Service and (b) the State shall provide reasonable assistance and cooperation to Atos in connection with any relocation or change described above.
- e. Atos may at any time change its Internet Service Provider (ISP) as may be necessary for Atos to supply the Services in the most appropriate manner and/or to best address the State's then current workload requirements. The State will be given advance written notice of any changes, which would affect its processing. An RFC will be processed if such changes result in increased Managed Hosting Service Fees.

Appendix B

Request for Change Form



Requestor:	Client:	Submitted:
Phone:	Fax:	Email:
Description of Change (attach any supporting documentation):		
Reason for Change:		
Requested Evaluation Date:		Requested Completion Date:
Priority (check one):	Impact (check one):	
<input type="checkbox"/> 1= Urgent <input type="checkbox"/> 2= High <input type="checkbox"/> 3= Medium <input type="checkbox"/> 4= Low	<input type="checkbox"/> 1= Top <input type="checkbox"/> 2= High <input type="checkbox"/> 3= Medium <input type="checkbox"/> 4= Low	
FOLLOWING TO BE COMPLETED BY Atos Service		Log Number:
Evaluation (include assessment of affected systems and components):		
Deliverables:		
Expected Start	Expected Completion Date:	
Evaluator:	Date:	
Summary of Charges:		
Billable to Cap: YES <input type="checkbox"/> NO <input type="checkbox"/>	If Billable, \$ /hour	Charge Number:

Final Approval

Atos Services Approval/Date:
Client Approval/Date (person authorized for expenditure of funds):
Purchase Order Number (REQUIRED if request is direct billable):

After Action Review:

Actual Change Date:	Completion: Yes <input type="checkbox"/> No <input type="checkbox"/>
Change Results (if partial explain or if not completed list reason):	

Attachment 1

State Provided Third Party Software:

Software
Louis
Sourcer

Attachment 2

State Provided Hardware:

Quantity	Description
1	DBSP and channels
2	Media Servers

Attachment 3

Attestation Regarding Prohibition on the Use of Illegal Immigrants

ATTACHMENT 3

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	Atos IT Solutions and Services, Inc.
EDISON VENDOR IDENTIFICATION NUMBER:	595

The Contractor, identified above, does hereby attest, certify, warrant, and assure 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.



CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

STEPHEN SMITH SVP Big Data / Cyber

PRINTED NAME AND TITLE OF SIGNATORY

7 Nov 2017

DATE OF ATTESTATION

Amendment Request

This request form is not required for amendments to grant contracts. Route a completed request, as one file in PDF format, via e-mail attachment sent to: Agsprs.Agsprs@tn.gov

APPROVED

CHIEF PROCUREMENT OFFICER

DATE

Agency request tracking #	33701-40919	
1. Procuring Agency	Department of Labor & Workforce Development	
2. Contractor	Atos IT Solutions and Services, Inc.	
3. Edison contract ID #	56931	
4. Proposed amendment #	1	
5. Contract's Original Effective Date	11/11/17	
6. Current end date	11/10/19	
7. Proposed end date	11/10/20	
8. Current Maximum Liability or Estimated Liability	\$ 2,558,326.20	
9. Proposed Maximum Liability or Estimated Liability	\$ 3,960,606.51	
10. Strategic Technology Solutions Pre-Approval Endorsement Request – information technology service (N/A to THDA)	<input type="checkbox"/> Not Applicable <input checked="" type="checkbox"/> Attached	
11. eHealth Pre-Approval Endorsement Request – health-related professional, pharmaceutical, laboratory, or imaging	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached	
12. Human Resources Pre-Approval Endorsement Request – state employee training service	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached	
13. Explain why the proposed amendment is needed	<p>The proposed amendment provides funds for a one-year extension to the current contract.</p> <p>The amendment will also provide an opportunity to update the contract's information security language to the current standard (Attachment 5).</p>	
14. If the amendment involves a change in Scope, describe efforts to identify reasonable, competitive, procurement alternatives to amending the contract.	N/A	

Agency request tracking #	33701-40919
Signature of Agency head or authorized designee, title of signatory, and date (the authorized designee may sign his or her own name if indicated on the Signature Certification and Authorization document)	



CONTRACT AMENDMENT COVER SHEET

Agency Tracking # 33701-40919	Edison ID 56931	Contract # 56931	Amendment # 1		
Contractor Legal Entity Name Atos IT Solutions and Services, Inc.			Edison Vendor ID 189689		
Amendment Purpose & Effect(s) One-year extension with updated security language					
Amendment Changes Contract End Date: <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO		End Date: 11/10/2020			
TOTAL Contract Amount INCREASE or DECREASE per this Amendment (zero if N/A):			\$ 1,402,280.31		
Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
18		\$831,976.00			\$831,976.00
19		\$1,289,562.80			\$1,289,562.80
20		\$1,137,927.55			\$1,137,927.55
21		\$701,140.16			\$701,140.16
TOTAL:		\$3,960,606.51			\$3,960,606.51
Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.			<i>CPO USE</i>		
Speed Chart (optional)		Account Code (optional)			

**AMENDMENT 1
OF CONTRACT 56931**

This Amendment is made and entered by and between the State of Tennessee, Department of Labor & Workforce Development, hereinafter referred to as the "State" and Atos IT Solutions & Services, Inc., hereinafter referred to as the "Contractor." For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said, undersigned contracting parties that the subject contract is hereby amended as follows:

1. Contract section C.1. is deleted in its entirety and replaced with the following:

C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed Three Million, Nine Hundred Sixty Thousand, Six Hundred Six Dollars and Fifty One Cents (\$3,960,606.51) ("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.

The Contractor is not entitled to be paid the maximum liability for any period under the Contract or any extensions of the Contract for work not requested by the State. The maximum liability represents available funds for payment to the Contractor and does not guarantee payment of any such funds to the Contractor under this Contract unless the State requests work and the Contractor performs said work. In which case, the Contractor shall be paid in accordance with the payment rates detailed in Section C.3. 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.

2. Contract section E.7. is deleted in its entirety and replaced with the following:

E.7. 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 or ensure 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. The obligations set forth in this Section shall survive the termination of this Contract.

3. The following is added as Contract section E.13.:

E.13. Contractor Hosted Services Confidential Data, Audit, and Other Requirements

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

- (1) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.
- (2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.
- (3) The Contractor and the Contractor's processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor's and Subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

- (4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of

discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

- (5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State
- (6) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

- (1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: <https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html>.
- (2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
- (3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

- d. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:
- (1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:
 - i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: **TWENTY-FOUR (24) HOURS.**
 - ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: **TWENTY-FOUR (24) HOURS.**
 - (2) The Contractor and any Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

4. Contract Attachment 5 attached hereto is added as a new attachment.

Required Approvals. The State is not bound by this Amendment until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

Amendment Effective Date. The revisions set forth herein shall be effective once all required approvals are obtained. All other terms and conditions of this Contract not expressly amended herein shall remain in full force and effect.

IN WITNESS WHEREOF,

ATOS IT SOLUTIONS AND SERVICES, INC.:

SIGNATURE

DATE

PRINTED NAME AND TITLE OF SIGNATORY (above)

TENNESSEE DEPARTMENT OF LABOR & WORKFORCE DEVELOPMENT:

JEFF MCCORD, COMMISSIONER

DATE

SAFEGUARDING CONTRACT LANGUAGE

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- (8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

- (9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.(10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information,

the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- (4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see [Exhibit 4, Sanctions for Unauthorized Disclosure](#), and [Exhibit 5, Civil Damages for Unauthorized Disclosure](#)). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See [Section 10](#)) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.