

SWC# 3021 Comprehensive Cloud Solutions
Contract Information and Usage Instructions

Specific instructions for **STS workstation consolidated executive branch agencies**, **non-consolidated executive branch agencies**, and **local governments** are broken out below on pages **3**, and **5**, and **6**.

Summary

Statewide contract 3021 is a NASPO cooperative contract between the State of Tennessee and four suppliers: Carahsoft, Insight, Strategic Solutions and SHI.

The scope of offerings includes Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) solutions including, but not limited to Amazon Web Services, Google Cloud Platform, and Microsoft Azure. Cloud professional services such as fixed-deliverable projects, application managed services, cloud solution assessments, or training for applicable solutions are also included. The following table shows which supplier offers which platform:

	AWS	GCP	Azure
Carahsoft	•	•	
Insight	•	•	•
SHI	•	•	•
Strategic	•	•	•

Contract Period:

	Carahsoft	Insight	Strategic	SHI
Start Date	9/1/2020	9/14/2020	5/23/2023	9/21/2020
End Date with All Renewals Executed	9/15/2026	9/15/2026	9/15/2026	9/15/2026

State Contact Information

Contract Administrator

Michael D. Gross, Category Specialist
 Central Procurement Office
Michael.D.Gross@tn.gov
 (615) 507-6227

Strategic Technology Solutions Contact

Chris Benson, Director of Business Operations
 Strategic Technology Solutions
Chris.Benson@tn.gov
 (615) 770-1126

Supplier Contact Information

Company Name: Carahsoft
Master Agreement #: AR2472
Edison Contract Number: 67955

Quote requests: NASPO@carahsoft.com

SOW requests: SMGNASPO@carahsoft.com

Colby Bender, Team Lead, Contracts Team

Colby.Bender@Carahsoft.com

(703) 889-9878

Company Name: Insight
Master Agreement #: AR2485
Edison Contract Number: 67958

Quote requests: TeamAshley2@insight.com

Ashley McDonald, Account Executive, Field Sales

Ashley.McDonald@Insight.com

(423) 368-9042

Company Name: Strategic Communications
Master Agreement #: AR2490
Edison Contract Number: 78633

Quote requests: naspo@yourstrategic.com

Justin Hampton, Account Executive

844-243-2053

Company Name: Software House International (SHI)
Master Agreement #: AR2488
Edison Contract Number: 67960

Quote requests: SoutheastTeamgov@shi.com

Nick Porco, Account Executive

Nick_porco@shi.com

629-401-8746

Inside Team Distribution:

Ryan Lee, Account Executive

ryan_lee@shi.com

615-390-2836

Lexi Ettman,

Inside Account Manager

lexi_ettman@shi.com

800-715-6055

Offerings

Each supplier has a reseller list which shows offerings that are currently available. These can be found on the NASPO websites listed below:

- Carahsoft – [https://www.naspo.valuepoint.org/portfolio/cloud-solutions-2016-2026/carahsoft-](https://www.naspo.valuepoint.org/portfolio/cloud-solutions-2016-2026/carahsoft-2)

[technology-corporation/](#)

- Insight - <https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/insight-public-sector-inc/>
- Strategic Communications - <https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/strategic-communications-llc/>
- SHI - <https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/shi-international-corp/>

Always ask each of the four suppliers for quotes to ensure the best price.

INSTRUCTIONS FOR STS WORKSTATION CONSOLIDATED EXECUTIVE BRANCH AGENCIES

If you wish to purchase a cloud solution not found on price lists, please contact Chris Benson at STS Business Operations with the request. STS Business Operations will review the request and work with the Contract vendors to determine if the requested solution is available through this contract.

ServiceNow

All purchases from these contracts must be purchased through [ServiceNow](#) unless prior written authorization received from Chris Benson or Emily Gibson to procure directly in Edison (see link below). https://tn.service-now.com/sp?id=sc_cat_item&sys_id=8775167a13826a009f84b6246144b071

An STS Endorsement is required if your agency has not procured the specific offering at some point in the past.

If you have an interest in purchasing Infrastructure-as-a-Service through this contract, please contact CloudTN@tn.gov or IT consolidated agencies may request a consultation with the CloudTN team through the ServiceNow request, "[CloudTN Consultation](#)".

Statements of Work

Please use a statement of work (SOW) when your purchase includes customized professional services. We have created a SOW template for your use, see Attachment 1 below.

Pick List

This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either in a SOW or printed on to the purchase order directly if no SOW is being used. STS Information Security will review the type(s) of data being hosted and will designate what additional applicable terms and conditions will apply to the purchase.

EULA Rider

Please be aware that when ordering from a new publisher, the supplier may require the State to agree to an End User License Agreement or other terms and conditions as part of the order. If the supplier requires the State to agree to additional terms and conditions for the order, a EULA Rider may need to be negotiated. Negotiations will be conducted between CPO Legal and the software publisher in question. Please email Michael Gross if this need arises. A EULA Rider template is included below as Attachment 2 for reference.

Justification

When entering your Edison requisition or ServiceNow procurement request for any order placed against this contract please attach brief justification documentation for audit purposes. Justification should include an explanation of the business need(s) being met by the requested solution and a description of the research the procuring agency performed to support the selection of the requested solution.

Software Waiver / Exception Process

Follow the steps below to request a waiver or exception to a cloud-based software (Software as a Service, SaaS) standard included in the Tennessee Enterprise Architecture.

1. Download the Waiver/Exception Request form here: <https://www.teamtn.gov/sts/planning-services/information-systems-planning/waiver---exception-process.html>
2. Complete the form electronically.
3. Email the completed form to AG_Standard_Products_List@tn.gov along with any additional information needed to support the Exception Request.

INSTRUCTIONS FOR NON-STIS WORKSTATION CONSOLIDATED EXECUTIVE BRANCH AGENCIES

Please contact the Contract vendors directly to inquire about the availability of a cloud solution for resale.

If you have an interest in purchasing Infrastructure-as-a-Service through this contract, please contact CloudTN@tn.gov.

Statements of Work

Please use a statement of work (SOW) when your purchase includes customized professional services. We have created a SOW template for your use, see Attachment 1 below.

Pick List

This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either in a SOW or printed on to the purchase order directly if no SOW is being used.

EULA Rider

Please be aware that when ordering from a new publisher, an End User License Agreement (EULA Rider) may need to be negotiated. Negotiations will be conducted between CPO Legal and the software publisher in question. Please email Michael Gross if this need arises. A EULA Rider template is included below as Attachment 2 for reference.

Justification

When entering your Edison requisition for any order placed against this contract please attach brief justification documentation for audit purposes. Justification should include an explanation of the business need(s) being met by the requested solution and a description of the research the procuring agency performed to support the selection of the requested solution.

INSTRUCTIONS FOR LOCAL GOVERNMENTS

Please contact the Contract vendors directly to inquire about the availability of a cloud solution for resale.

Statements of Work

We have created a SOW template for State agencies to use in the event their purchase includes customized professional services. You may be able to modify this template for your uses if you so wish - see Attachment 1 below.

Pick List

This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either in a SOW or printed on to the purchase order directly if no SOW is being used.

EULA Rider

Please be aware that when ordering from a new publisher, an End User License Agreement (EULA Rider) may need to be negotiated. We have created a EULA Rider template for State agencies if the need arises. You may be able to modify this template for your uses if you so wish - see Attachment 2 below.



RSWC #3021 NASPO Cloud Solutions

Department of Finance & Administration – STS

Statement of Work
SOW ID SFT# xxxx

For

[Insert Project Title]

[SOW Start Date]

Contents

1.1 Project Title	9
1.2 Background	9
1.3 Reference to other applicable documents	9
1.4 Definitions	10
2.0 STAFFING AND ROLES	10
2.1 State Staff and Roles:	10
2.2 Contractor Staff and Roles:	11
3.0 PROJECT REQUIREMENTS AND DELIVERABLES	11
3.1 Contractor Requirements and Deliverables	11
3.2 State Tasks and Responsibilities	12
3.3 Exclusions	12
4.0 DELIVERABLE ACCEPTANCE	12
5.0 COST CRITERIA	12
5.1 Payment Methodology	12
5.4 State Billing Address	13
6.0 ESTIMATED TIMELINE AND PERIOD OF PERFORMANCE	13
7.0 PROJECT MANAGEMENT (IF APPLICABLE)	13
8.0 ADDITIONAL STATE POLICIES AND STANDARDS	13
9.0 KEY ASSUMPTIONS	14
10.0 SOW Revision Procedure	14
11.0 SOW Termination	15

1.0 Statement of Work

1.1 *Project Title*

This Statement of Work (SOW) is being executed between *[insert Contractor name]* (“Contractor”) and *[Insert Agency]* (“State”) for *[insert a brief description of the project]*, effective as of *[Insert Effective Date]* (the “SOW Effective Date”).

- *Update/include this subcontractor language below in the event of this SOW project utilizes subcontractors.*

[Subcontractor name] (xx) shall act as a “Subcontractor” to *[Contractor Name]* (“Contractor”) to perform the requested professional services. When references are made to the “Contractor” performing work under this SOW, this shall be construed to mean that the work is performed by Subcontractor. However, the Subcontractor is not a signatory to this SOW, and the Contractor shall be fully responsible for the successful execution of all requested services.

This SOW constitutes an Order under applicable Participating Addendum between the Contractor and the State, via Edison Contract # *xxxxx* (the “Contract”) and incorporates by reference the terms and conditions, specifications, and other incorporated contract documents of the Contract. In case of any conflict between this SOW and the Contract, the Contract shall prevail.

1.2 Background

- *Describe the history of your project and the prior events that brought you to this SOW*

1.3 Reference to other applicable documents

The following documents are hereby incorporated by reference into this SOW:

- *List any pertinent documents or supporting materials pertaining to the SOW, if any, otherwise write “None”.*
- *(TBD) Attachment 1 – Technical Proposal*
- *(TBD) Attachment 2 – Cost Proposal*
- *(TBD) Attachment 3 – Security Requirements Rider*
- *(TBD) Attachment 4 - NASPO Master Agreement Rates*

1.4 Definitions

1.5 Security, Audit, and Other Requirements –

a. Security Requirement Rider

The State’s confidential data and security requirements (“Requirements”) are contained in the NASPO Comprehensive Cloud Solutions Participating Addendum (PA) and have been agreed to by the participating Contractors to comply with during a SOW project.

To bring attention to the specific Requirements the Contractor shall provide and comply with during the SOW project in question, a Security Requirement Rider will be included as an attachment to this SOW.

The Security Requirement Rider, SOW Attachment X contains the full version of the Contractor Hosted Services Confidential Data, Audit, and Other Requirements terms and conditions included in the NASPO Comprehensive Cloud Participating Addendum (PA).

Additional Operational Security Requirements are listed in Attachment X Section 2.

NOTE: The applicable security Requirements will be dependent upon the type(s) of data associated with the project requirements and deliverables outlined in this SOW.

b. The SOW shall limit contractor resources to US-based (onshore) resources only.

2.0 STAFFING AND ROLES

2.1 State Staff and Roles:

Following are the STS staff to assist with the Project effort and have decision-making authority, including approval of changes, report, documentation, and deliverables.

Name	Project Role	Responsibilities
[Name]	STS Executive Sponsor	Provides high-level vision and oversight for the duration of the Project.
[Name]	STS Project Director	Provides enterprise-level guidance and oversight for the duration of the Project. Coordinate Deliverable approvals and recommend invoice payments. Contractor’s main point of contact throughout the Project.
[Name]	STS Operations Project Manager	Oversees day-to-day project activities and consults with STS Agency Project Director and STS Agency Project Team, including technical and program staff, for project execution. Monitors and reports Project progress to the STS Agency Project Team. Proactively works with the Contractor to identify the risks and issue resolution.
[Name]	STS Agency Product Owner	Acts as key decision maker to clarify business and policy questions, review and approve system requirements and design

		documentation in adherence with the approved Project Work Plan.
[Name]	STS Technical Resource	Responsible for technical design review and approval, environment provision, allocation, and usage.

2.2 Contractor Staff and Roles:

- *Who from the Contractor will have decision-making authority, including approval of changes, report, documentation, and deliverables?*
- *Contractor staff (if any) to assist with the project effort.*
- *Individuals key to the project and detail their roles and responsibilities.*

Contractor's Point of Contact:

Name:

Address:

City:

State & Zip

Phone:

Cell:

Email:

Subcontractor's Point of Contact:

Name:

Address:

City:

State & Zip

Phone:

Cell:

Email:

3.0 PROJECT REQUIREMENTS AND DELIVERABLES

3.1 Contractor Requirements and Deliverables

3.1.1 Requirements:

- *Tasks to be performed and any additional Contractor qualifications for specialized projects*
- *Any known non-standard work schedule tasks*
- *Location(s) where project work is required to be performed or may be performed, including the use of onsite, offsite, and offshore resources at the procuring State's discretion*
- *Include tasks that do not result in specific deliverables (i.e. project management)*

- *Include any security requirements from Special Terms and Conditions, Section 13 of the Contract that are applicable to this SOW.*

3.1.2 Deliverables

- *Describe the Deliverables to be provided under this SOW, including the estimated delivery dates. If no Deliverables, state "none."*

3.2 State Tasks and Responsibilities

- *Include tasks to be performed by the State*
- *Precise definition of all hardware, software, data services, and facilities the State will provide*

3.3 Exclusions

Describe:

- *Tasks which are not part of the scope of this project*

4.0 DELIVERABLE ACCEPTANCE

Insert acceptance language from appropriate NASPO Cloud PA depending on which Contractor is selected.

5.0 COST CRITERIA

5.1 Payment Methodology

The State shall compensate the Contractor for actual work performed under the [Time and Materials or Fixed Fee] Payment Methodology. The Contractor will invoice the State, no more often than monthly increments, in arrears, in accordance with the Table listed below:

[Insert payment methodology table. Examples of payment tables can be found in the optional language section at the end of the SOW template.]

Rates should be equal to or less than the rates agreed to in the Contractor's Master Agreement.

5.2 Travel and Expenses

The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

5.3 SOW Monetary Cap

Check one of the following to apply to this SOW:

- This SOW is a fixed fee SOW. The total charges under this SOW is [_____] dollars (\$____) [specify SOW monetary cap] for the performance of the work as set forth in this SOW.

- This SOW is a time and materials SOW. The total charges under this SOW is [_____] dollars (\$____) [specify SOW monetary cap] for the performance of the work as set forth in this SOW (the “SOW NTE Amount”). The State shall compensate the Contractor for actual work performed, in an amount not to exceed the SOW NTE Amount. The State shall not be obligated to pay for, and the Contractor shall not be obligated to perform, work under this SOW in excess of the SOW NTE Amount unless and until the parties execute a written revision to this SOW to increase such SOW NTE Amount.

5.4 State Billing Address

Insert the applicable State billing address.

6.0 ESTIMATED TIMELINE AND PERIOD OF PERFORMANCE

Project must begin no later than [Month, Year] and be completed by [Month, Year].

Optional Milestone Table

Milestone	Date

7.0 PROJECT MANAGEMENT (IF APPLICABLE)

Describe what will be required as far as project management, which reports will be required, how often these reports will be required, and what must be submitted to the State.

8.0 ADDITIONAL STATE POLICIES AND STANDARDS

Specifically reference any additional state policies and standards that would apply, to the extent applicable to Contractor in its performance of the work under the Order. If none, write “none”.

- *Insert any other relevant links to the latest versions of the policies, standards and environment*

9.0 KEY ASSUMPTIONS

Identify any additional State or contractor assumptions

If additional sections are required for your specific project, please leave the above section numbering as it is and add your new sections here as 10.0, 11.0 etc.

10.0 SOW Revision Procedure

The State may request necessary changes to the deliverables and requirements due to policy or operational changes during the SOW term. The Contractor shall address these necessary changes as per the SOW revision procedures described in this section.

- 10.1 The State shall provide to the Contractor a written request for changes. After receipt of the written request, the Contractor shall respond to the State with a written proposal for implementation of the change. The written proposal must include the following:
- a) Complete description of the work to be performed as the Contractor understands it,
 - b) Work plan showing the major activities needed to complete the necessary change, including adjustment to the schedule and tasks required, and
 - c) Provide a “not to exceed” total cost for the work in question. The State shall pay no more than, and the Contractor will not be required to provide services in excess of, this cost for the services engagement. The Contractor shall provide supporting documentation which lists the number of hours and materials, if applicable, that constitute the “not to exceed” cost.
- 10.2 The State shall review the Contractor’s written proposal and approve or request additional clarification for approval. If approved, the agreed to changes will be documented in the State’s standard SOW revision template.
- 10.3 The Contractor and the State shall sign the SOW revision template. Once executed by the Contractor and the State, the SOW, shall be binding to both parties. and it shall constitute an revision between the SOW parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this SOW.
- 10.4 The SOW revision shall not conflict with, modify, or delete the terms and conditions of the SOW or Contract. In the event of a conflict or ambiguity between the Contract, SOW, and this SOW amendment, the Contract, then the SOW shall prevail, in that order.
- 10.5 SOW revisions shall not contain any other legal terms and conditions that modify, contradict, or supplement the terms of the SOW or Contract. Any such terms and conditions

contained in a SOW revision shall be void, invalid, and unenforceable against the State.

11.0 SOW Termination

- 11.1 The applicable Purchasing Entity may terminate a SOW for convenience without cause and for any reason. The Purchasing Entity shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the Purchasing Entity and for services completed in accordance with the terms of the SOW as of the termination date. In no event shall the Purchasing Entity be liable to the Contractor for compensation for any goods neither requested nor accepted by the Purchasing Entity or for any services neither requested by the State nor performed by the Contractor in accordance with the terms of the applicable Order. In no event shall the Purchasing Entity's exercise of its right to terminate the applicable SOW for convenience relieve the Contractor of any liability to the Purchasing Entity for any damages or claims arising under the SOW.
- 11.2 If a party to a SOW ("SOW Breaching Party") fails to properly perform its obligations under the SOW, or if a party to a SOW materially violates any terms of the applicable SOW ("SOW Breach Condition"), the other party to the SOW ("SOW Non-breaching Party") may provide written notice to the SOW Breaching Party specifying the SOW Breach Condition. If within thirty (30) days of notice, the SOW Breaching Party has not cured the SOW Breach Condition, the SOW Non-breaching Party may terminate the applicable SOW. In the event the SOW Non-breaching Party is the Purchasing Entity, the Purchasing Entity may withhold payments under the applicable SOW in excess of compensation for completed services or provided goods. The SOW Breaching Party shall not be relieved of liability to the SOW Non-breaching Party for damages sustained by virtue of any breach of the applicable SOW, and the SOW Non-breaching Party may seek other remedies allowed at law or in equity for breach of the applicable SOW.
- 11.3 If any SOW is terminated pursuant to this Section, this Contract shall continue to apply to all SOWs that have not been terminated.
- 11.4 This section shall not limit the State's right to terminate the Contract for convenience or cause in accordance with Sections 4 and 5 of the Standard Terms and Conditions, above.

This SOW will not be effective, and Contractor shall not commence services hereunder, until it is approved and signed by Contractor and the Participating Entity.

In witness whereof, the parties have executed this SOW as of the last date of execution of the signatories below.

<i>[Insert State Purchasing Agency]</i>	<i>[Contractor Name]</i>
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

Security Requirement Rider
Applicable Security Terms and Conditions
and Operational Requirements

Internal Instructions: *After the STS Security team determines what requirements are required for a specific SOW, this attachment will be revised, through a subtractive process, to contain only the corresponding full version text of the Pick List requirement in SOW Section 1.4 and will then be attached to the NASPO Cloud SOW. (Delete instructions before adding the Attachment to the SOW)*

This Security Requirement Rider contains the full version text of the data confidentiality and data security terms and conditions found in the NASPO Comprehensive Cloud PA Section, Contractor Hosted Services Confidential Data, Audit, and Other Requirements that shall be applicable for this SOW.

These terms and conditions are also located in each of the NASPO Comprehensive Cloud Contractor's Participating Addendum (PA).

Please note pre-existing global security language exists in the resellers PA; therefore, it is unnecessary to repeat the language in this rider.

1. 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 Estimated Liability of this Contract.

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

Contractor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges ("MARS-E") controls.

(a) If the order will involve CJIS data, or FTI data then the following shall apply in lieu of section 14.a.(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. No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Estimated Liability of this Contract.

(b) If the order will contain FTI data, the following sentence also applies to section 14.a.(3)(a) (FedRAMP) language above:

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

(c) If the order will involve CMS data, the following sentence also applies to section 14.a.(3)(a) language above:

Contractor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges (“MARS-E”) controls.

(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.

(7) If the order will involve PCI data, the following shall apply: Contractor shall be certified to host Payment Card Industry (“PCI”) data in accordance with the current version of PCI DSS (“Data Security Standard”), maintained by the PCI Security Standards Council.

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. 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: The applicable RPO will be defined in each Order.

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: The applicable RTO will be defined in each Order.

2. The Contractor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

3. The Contractor shall have the ability to provide base level protection against Layer 3 and Layer 4 Distributed Denial of Service volume based and protocol attacks such as SYN, UDP, and ICMP floods, DNS amplification and reflection attacks.

4. The contractor shall have the ability to provide addition mitigation against Layer 7 Distributed Denial of Service attacks such as HTTP floods, WordPress XML-RPV Floods and Slowloris attacks.

- d. In the event of a cyber breach, the Contractor will allow the State to communicate directly with the Contractor's technical staff and any forensics experts who are assisting the Contractor with the breach analysis.

2. ADDITIONAL OPERATIONAL SECURITY REQUIREMENTS:

(The following requirements are not contained in the terms and conditions of the PA but will be in effect and binding for the duration of this SOW.)

The following operational security requirements are applicable to this SOW:

2.1 The Contractor shall use STS resources when they use State systems.

2.2 The SOW shall limit contractor resources to US-based (onshore) resources only

2.3 The Contractor shall use State issued devices, refer to Section XXX

2.4 The Contractor shall communicate using their State-provided email account and other State communication tools.

2.5 Contractor shall utilize STS's Incident Response ticking system, ServiceNow.

2.6 Contractor shall utilize STS's current provisioning/de-provisioning scripted processes.

2.7 All updated OS images shall be approved by STS's Security Team prior to usage.

2.8 State Tasks & Responsibilities

- (1) Precise definition of all hardware, software, data services, and facilities the State will provide.
- (2) The State shall provide workstations to all individuals supporting the contract. The Contractor shall be responsible for recompensating expenses to the State of any State-issued equipment not returned to the State.
- (3) STS Project Sponsor will have overall responsibility and authority for driving all program decisions, reviewing, and approving all deliverables, facilitating discussion and communication among all parties as needed, and securing any required State or third-party resources.
- (4) Provide recommendations for an operating model that would address state security requirements and practices.

- (5) Participate and/or facilitate participation among the STS groups in all meetings and project communications to provide the necessary inputs required to complete the required deliverables.
- (6) Commit the necessary resources and project management involvement to support the program.
- (7) Be responsible for providing resources with access to individuals and tools necessary for Contractor to perform the requested services in accordance with State policies and least privileges.
- (8) Provide escalation support to resolve related issues.
- (9) Provide necessary approvals required for resolving a service outage, per the change management processes established by STS.
- (10) Provide timely support in validation and testing of Incident resolution to complete any fixes to data and/or program to support the closure of incident tickets.
- (11) Establish the connectivity needed from STS' Data Centers to AWS and Azure Infrastructure.
- (12) Notify the Contractor of upcoming planned maintenance activities for any components in the Cloud.

Optional SOW Language:

- Section 3 requirement language:
 - Acceptance testing of Functional Deliverables during UAT will involve the validation of each Functional and Successfully Operating Deliverable against the Approved State Specifications. The acceptance period for the Functional Operating Deliverable will be **10** business days. If the Functional and Successfully Operating Deliverable conforms to the Approved State Specifications, it will be accepted. If not, then any Material Nonconformities will be:
 - X.** fed by Subcontractor into list of identified defects or product backlog and;
 - X.** prioritized by the State and mutually agreed by both Parties to be addressed as part of the scope of services defined in the SOW or deferred for future consideration. Contractor/Subcontractor’s correction efforts will be made on a time and materials basis. If Contractor/Subcontractor does not receive notice identifying a Material Nonconformity from State during acceptance period or State begins using the Functional and Successfully Operating Deliverable in a production environment, or the acceptance period expires, the Functional and Successfully Operating Deliverable shall be deemed to be accepted.

- Section 5.1 Payment Methodology:
Time and Material payment methodology:

Table 1: Hourly Rate Card

[Insert CONTRACTOR HOURLY RATE CARD details in Table below]

<i>Position Description</i>	<i>NASPO SKU</i>	<i>Hourly Rate*</i>	<i>Number of Hours</i>	<i>Cost</i>
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of

				Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
Position Name	#	\$NUMBER /HR	#	Rate x # of Hours
TOTAL Fees				\$0.00

Fixed Fee payment methodology:

Milestone Payment Methodology

The Milestone (Not To Exceed Fixed Fee) Methodology will be used as indicated in the tables below.

The Contractor shall provide a rate card by which the Milestone NTE Fixed Fees will be calculated for use in this SOW.

(1) Deliverable Table 1. See requirements listed in Section 3 of the SOW.

Milestone NTE Deliverable 1 - [Description Title]				
Position Description(s)	NASPO SKU	Hourly Rate	Number of Hours	Cost
CLASSIFICATION POSITION	#	\$NUMBER /HR	#	Rate x # of Hours
CLASSIFICATION POSITION	#	\$NUMBER /HR	#	Rate x # of Hours
<u>TOTAL</u>				\$0.00

(2) Deliverable Table 2. See requirements listed in Section 3 of the SOW.

Milestone NTE Deliverable 2 - [Description Title]				
Position Description(s)	NASPO SKU	Hourly Rate	Number of Hours	Cost
CLASSIFICATION POSITION	#	\$NUMBER /HR	#	Rate x # of Hours
CLASSIFICATION POSITION	#	\$NUMBER /HR	#	Rate x # of Hours
TOTAL				\$0.00

Fixed Fee payment methodology:

Table 1: Monthly Payment Schedule

[Insert CONTRACTOR MONTHLY PAYMENT SCHEDULE details in Table below]

January 2023	\$NUMBER
February 2023	\$NUMBER
March 2023	\$NUMBER
April 2023	\$NUMBER
May 2023	\$NUMBER
June 2023	\$NUMBER
July 2023	\$NUMBER
August 2023	\$NUMBER
September 2023	\$NUMBER
October 2023	\$NUMBER
November 2023	\$NUMBER
December 2023	\$NUMBER

Fixed Fee Rates should be equal to or less than the rates agreed to in the Contractor’s Master Agreement. Contractor is responsible for providing the NASPO Master Agreement rates as an attachment X to the SOW for financial audit purposes.

- Section 7 Project Management language:
 - The State reserves the right to request personnel changes to the Contractor project team if it is determined that performance does not meet State’s expectations. If personnel changes are necessary, the Contractor shall replace assigned personnel with equal or higher skills and meets the requirements defined in section 3 to the personnel

who are replaced. The Contractor must submit resumes of replacement personnel within five (5) business days of State notification.

- Section 9 Key Assumption language:
 - The Contractor shall procure a State approved laptop device. A basic State image shall be installed on the device prior to shipment. Once received by the Contractor, the State will remotely install all required software applications and tools to be in compliance with the State's Information Security Policy. At the end of the SOW, the Contractor shall permit the State to remotely access the devices in order to delete all data from the devices. Cost of the devices must be included as a part of the monthly services fee.

Section 1.5 Security, Audit, and Other Requirements Language:

The SOW shall limit contractor resources to US-based (onshore) resources only