State of Georgia
Statewide Standard Contract Form

Solicitation Title	Solicitation Number	Contract Number
Networking Equipment and Related Services	**99999-SPD0000219**	**99999-SPD-SPD0000219-0008**

1. This Contract is entered into between the Agency and the Supplier named below:

Agency's Name
Department of Administrative Services
(hereafter called Agency)

Supplier's Name
Juniper Networks (US), Inc.
(hereafter called Supplier)

2. Contract to Begin:	Date of Completion:	Renewals:
11/18/2024	11/17/2026	Five (5) one (1) year renewal option(s)

3. Performance Bond, if any:	Other Bonds, if any:
N/A	**N/A**

4. Authorized Person to Receive Contract Notices for Agency:	Authorized Person to Receive Contract Notices for Supplier:
McCall Ginsberg, Deputy General Counsel	Roxanne Bieniek, Sr. Mgr. Contracts Administration

5. The parties agree to comply with the terms and conditions of the following attachments which are by this reference made a part of the Statewide Contract:

Attachment 1: **Statewide Contract for Goods and Ancillary Services**
Attachment 2: **Solicitation (referenced above)**
Attachment 3: **Supplier's Final Response**
Attachment 4: **State of Georgia, DOAS, Data Security Terms & Conditions**
Attachment 5: **JUNIPER PURCHASE AND LICENSE AGREEMENT as modified by the parties and attached**.

IN WITNESS WHEREOF, this Contract has been executed by the parties hereto.

6. Juniper Networks (US), Inc.

Supplier

Supplier's Name *(If other than an individual, state whether a corporation, partnership, etc.)*

Signed by:
T. Bu

By *(Authorized Signature)*	Date Signed
Tim Bunting	8/22/2024

Printed Name and Title of Person Signing
Assoc. General Counsel Sr. Dir.

Juniper Networks
Legal Department
Zachary Mills
Approved As To Form
Zachary Mills

Address
2251 Corporate Park Drive, Herndon, VA 20171

7.

Agency

Agency Name
Department of Administrative Services

By *(Authorized Signature)*	Date Signed
Jim Barnaby	9/24/2024

Printed Name and Title of Person Signing
Jim Barnaby, Deputy Commissioner, DOAS SPD

Address
200 Piedmont Avenue, S.E., Suite 1804W
Atlanta, GA 30334-9010

STATE OF GEORGIA
STATEWIDE CONTRACT
Attachment 1
Contract Terms and Conditions for Goods and Ancillary Services

A. DEFINITIONS AND GENERAL INFORMATION

1. Definitions. Definitions and acronyms are set forth in the eRFP in Attachment I "Comprehensive List of Definitions of Terms and Acronyms". Such terms will apply to the Contract and all documents incorporated unless a different meaning is otherwise assigned herein to specific terms. The following words shall be defined as set forth below:

(i) "**Agency"** means the Department of Administrative Services of the State of Georgia.

(ii) **"Awarded Item Schedule"** means the summarizing document, if any, listing the goods and services as awarded and may also denote the Supplier providing such goods and services.

(iii) **"Contract"** or **"Statewide Contract"** means the agreement between the Agency and the Supplier as defined by the Statewide Contract Form and its incorporated documents. This Contract may be executed in any number of counterparts, each of which shall be deemed to be an original, but all such counterparts shall together constitute one and the same Contract. The parties agree to conduct transactions by electronic means as provided under O.C.G.A. § 10-12-1 et seq. Electronic signatures complying with O.C.G.A. § 10-12-1 et seq., as amended from time-to-time, or other applicable law, shall be deemed original signatures for purposes of this Contract. Notwithstanding the foregoing, email signature blocks do not constitute signatures for the purpose of executing contracts and email communications do not constitute contracts; however, transmission by telecopy, electronic mail, or other transmission method of an executed counterpart of this Contract will constitute due and sufficient delivery of such counterpart.

(iv) **"Supplier"** means the provider(s) of the goods and services under the Statewide Contract.

(v) **"Cloud Services"** shall mean the duties and tasks undertaken by the Supplier to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Supplier online software applications identified herein, and to related services, such as Supplier hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Cloud Service solution.

(vi) **"Cloud Support"** includes provision of ongoing updates and maintenance for the Supplier online software applications, and as may be specified herein, consulting, training, and other support Services as provided by the Supplier for cloud tenants receiving similar cloud Services.

(vii) **"Purchase Instrument"** means the documentation issued by the Agency or User Agencies to the Supplier for a purchase of goods and services in accordance with the terms and conditions of the Statewide Contract. The Purchase Instrument should reference the Statewide Contract and may include an identification of the items to be purchased, the delivery date and location, the address where the Supplier should submit

the invoices, and any other requirements deemed necessary by the Agency or User Agencies.

(viii) **"Response", "Supplier's Response" or "Final Response"** means the Supplier's submitted response to the RFX, including any modifications or clarifications accepted by the Agency.

(ix) **"RFX"** means the Request for Proposal, Request for Bid, or other solicitation document (and any amendments or addenda thereto) specifically identified in the Statewide Contract Form that was issued to solicit the goods and/or services that are subject to the Statewide Contract.

(x) **"Services"** shall include administration, distribution, installation, configuration, support, training, and professional services as further described in the RFX.

(xi) **"State"** means the State of Georgia, the Agency, User Agencies, and any other authorized state entities issuing Purchase Instruments against the Statewide Contract.

(xii) **"Statewide Contract Form"** means the document that contains basic information about the Statewide Contract and incorporates by reference the applicable Contract Terms and Conditions, the RFX, Supplier's Response to the RFX, the final pricing documentation for goods and services and any mutually agreed clarifications, modifications, additions, and deletions resulting from final contract negotiations. No objection or amendment by a Supplier to the RFX requirements or the Statewide Contract shall be incorporated by reference into this Statewide Contract unless the Agency has accepted the Supplier's objection or amendment in writing. The Statewide Contract Form is defined separately and referred to separately throughout the Statewide Contract Terms and Conditions as a means of identifying the location of certain information. For example, the initial term of the Statewide Contract is defined by the dates in the Statewide Contract Form.

(xiii) **"State Entity"** means the State of Georgia entity identified in the Contract Form to contract with Supplier for the services identified in the Contract.

(xiv) **"User Agency"** or **"User Agencies"** means any offices, agencies, departments, boards, bureaus, commissions, institutions, or other entities of the State of Georgia entitled to or required to make purchases from this Statewide Contract.

2. **Certified Source of Goods and Services.** Pursuant to Section 50-5-57 of the Official Code of Georgia Annotated (O.C.G.A.), the Agency hereby certifies the Supplier as a source of supply to the User Agencies of the goods and services identified in this Statewide Contract. Orders shall be placed individually and from time to time by the User Agencies. The execution of this Statewide Contract only establishes the Supplier as an authorized source of supply by the Agency and creates no financial obligation on the part of the Agency.

3. **Priority of Contract Provisions**. Any pre-printed contract terms and conditions included on Supplier's forms or invoices shall be null and void. Notwithstanding anything to the contrary herein, the State shall not be subject to any provision included in any terms, conditions, or agreements appearing on Supplier's or a Subcontractor's website or any provision incorporated into any click-through or online agreements unless that provision is specifically incorporated in full into this Contract.

4. **Reporting Requirements.** Supplier shall provide all reports required by the RFX. In addition, unless otherwise provided in the RFX, Supplier shall keep a record of the purchases made pursuant to the Statewide Contract and shall submit a quarterly written report to the Agency.

B. DURATION OF CONTRACT

1. **Contract Term.** The Statewide Contract shall begin and end on the dates specified in the Statewide Contract Form unless terminated earlier in accordance with the applicable terms and conditions. Pursuant to O.C.G.A. Section 50-5-64, this Statewide Contract shall not be deemed to create a debt of the State for the payment of any sum beyond the fiscal year of execution or, in the event of a renewal, beyond the fiscal year of such renewal.

2. **Contract Renewal.** The Agency shall have the option, in its sole discretion, to renew the Statewide Contract for additional terms on a year-to-year basis by giving the Supplier written notice of the renewal decision at least sixty (60) days prior to the expiration of the initial term or renewal term. Renewal will depend upon the best interests of the State, funding, and Supplier's performance. Renewal will be accomplished through the issuance of a Notice of Award Amendment. Upon the Agency's election, in its sole discretion, to renew any part of this Statewide Contract, Supplier shall remain obligated to perform in strict accordance with this Statewide Contract unless otherwise agreed by the Agency and the Supplier.

3. **Contract Extension.** In the event that this Statewide Contract shall terminate or be likely to terminate prior to the making of an award for a new contract for the identified goods and services, the Agency may, with the written consent of Supplier, extend this Statewide Contract for such period as may be necessary to afford the State a continuous supply of the identified goods and services.

C. DESCRIPTION OF GOODS AND SERVICES

1. **Specifications in Bidding Documents.** The Supplier shall provide all goods, services, and other deliverables in compliance with the specifications contained in the RFX and the terms of the Statewide Contract, plus those equipment, services and deliverables as may additionally be described in the Response.

2. **Product Shipment and Delivery.** All products shall be shipped F.O.B. destination. Destination shall be the location(s) specified in the RFX or any provided Purchase Instrument. All items shall be at the Supplier’s risk until they have been delivered and accepted by the receiving entity. All items shall be subject to inspection on delivery. Hidden damage will remain the responsibility of the Supplier to remedy without cost to the User Agencies, regardless of when the hidden damage is discovered.

3. **Non-Exclusive Rights.** The Statewide Contract is not exclusive. The Agency reserves the right to select other Suppliers to provide goods and services similar to goods and services described in the Statewide Contract during the term of the Statewide Contract. User Agencies may obtain similar goods and services from other Suppliers upon prior approval of the Agency, which approval shall be made at the sole discretion of the Agency when it is deemed to be in the best interests of the State, and shall be conclusive.

4. **No Minimums Guaranteed.** The Statewide Contract does not guarantee any minimum level of purchases.

5. **Orders.** Any Order placed by a User Agency in the State of Georgia for a Good or Service available under this Contract shall be deemed to be a sale (and governed by the prices and

other terms and conditions) under this Contract unless the parties to the Order agree in writing that another contract or agreement applies to such Order.

6. Software and Specifications. The Supplier shall provide all software ("Software") in strict compliance with the descriptions and representations as to the Software (including performance, capabilities, accuracy, completeness, characteristics, specifications, configurations, standards, functions, and requirements) which appear in the RFX and the terms of the Contract.

7. Software Licenses. Supplier shall provide Software licenses ("Licenses") in compliance with the specifications contained in the RFX and the terms of the Contract. To the extent permitted and/or required by the Software publishers of any Software provided hereunder, Supplier hereby grants an revocable, nonexclusive, non-transferable, fully paid up, royalty-free license to use, execute, maintain, reproduce, modify, display, and perform copies (as described below) of Software and accompanying documentation in accordance with the licensing capacity (if any) specified in the RFX and or applicable Purchase Instrument. The State Entity may copy the Software as necessary to efficiently utilize the Software, such rights shall include copying rights granted to "owners of copies" under federal copyright laws of the United States, plus copying:

(i) For backup, archive, or emergency restart purposes;
(ii) For disaster recovery and disaster recovery testing purposes;
(iii) To migrate the Software for use on other computers and/or hardware; and
(iv) To store the Software at any off premise location which the State Entity uses for storage purposes.

If the Supplier is acting as a reseller of the Software, the Supplier must provide the Licenses, as required by the Software publishers, to the State Entity and shall coordinate with any negotiations of such Licenses as may be conducted between the State Entity and the Software publishers. All licenses provided hereunder shall remain in effect in accordance with the Software License Agreement.

Unless expressly authorized in writing, or except to the extent transfer may not be restricted under Georgia Law, the State shall not: (i) directly or indirectly decompile, disassemble, reverse engineer, modify, unbundle, or create derivative works based on any Software; (ii) remove, modify, or conceal any product identification, copyright, or confidential notices or other marks; or (iii) use or fail to restrict use of the Software in violation of applicable law.

Warranty. Juniper will provide Software with commercially reasonable care in material conformance with the applicable descriptive content.

Additional Software Terms.

(i) Supplier grants the State a license to use Software updates made available as part of the applicable Services for such Software or, if applicable, Hardware. The terms and conditions applicable to the Software also apply to any update of that Software.

(ii) The State may use the Software on any device that supports it, except for operating system Software: (i) included in the purchase of the Hardware; or (ii) if licensed and purchased separately, only on the replacement Hardware.

(iii) In the limited event that licensed Software includes source code, (either as part of the Software or made available separately by Supplier, or is ancillary to the use of Software), such source code is provided "as-is", without any warranty and for internal use only unless expressly licensed otherwise by Supplier.

8. **Services and other Deliverables.** Supplier shall provide Services and other deliverables in compliance with the specifications contained in the RFX and the terms of the Contract to include SOW if applicable.

9. **Product Shipment and Delivery.** All products shall be provided as required by the provisions of the RFX. Unless the RFX requires otherwise, all products shall be made available either by online download or shall be shipped F.O.B. destination. Destination shall be the location(s) specified in the Purchase Instrument. All items shall be at the Supplier's risk until they have been delivered and accepted by the receiving entity. All items shall be subject to inspection on delivery. Hidden damage will remain the responsibility of the Supplier to remedy without cost to the State Entity, regardless of when the hidden damage is discovered.

10. **Cloud Services Terms and Conditions.** For the purpose of this RFX "Cloud Services" encompasses Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service as it pertains to Network-as-a-Service. Nothing in this subsection shall supersede the provisions of the Data Security Terms and Conditions contained in Attachment 4. If any of the terms contained in this subsection conflict with those of the Data Security Terms and Conditions contained in Attachment 4 the Data Security Terms and Conditions shall govern.

    If the Services include Infrastructure as a Service, Network as a Service, Platform as a Service, Infrastructure as a Service, or Software as a Service, the following terms and conditions apply:

    (i) ACCESS AND USE OF CLOUD SERVICES:

    a. Supplier grants the Authorized User a personal non-transferable and non-exclusive right to use and access, all Cloud Services and other functionalities or services provided, furnished or accessible under this Agreement. The Authorized User may utilize Cloud Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The Authorized User is authorized to access Authorized User Data and any Supplier-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the Authorized User Data. This shall include the right of the Authorized User to, and access to, Cloud Support without the Supplier requiring a separate maintenance or support agreement. User access to the Cloud Services shall be routinely provided by the Supplier and may be subject to a more specific Service Level Agreement (SLA) or Scope/Statement of Work (SOW) agreed to in writing by the parties. The Authorized User also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly, or reverse compilation to derive a source code equivalent to the Cloud Services or any portion thereof. Use of the Cloud Services to perform services for commercial third parties (so- called "service bureau" uses) is not permitted, but the Authorized User may utilize the Services to perform its governmental functions. If the Cloud Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time by mutual agreement between Supplier and Authorized User All Cloud Services and information designated as "confidential" or

"proprietary" shall be kept in confidence except as may be required by the Georgia Open Records Act, O.C.G.A. § 50-18-70, *et. seq.*

b. The Authorized User's access license for the Cloud Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Supplier or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Cloud Services. Any Cloud Services or technical and business information owned by Supplier, or its Suppliers or licensors made accessible or furnished to the Authorized User shall be and remain the property of the Supplier or such other party, respectively. Supplier has a limited, non-exclusive license to access and use the Authorized User Data as provided to Supplier, but solely for performing its obligations under this Agreement and in confidence as provided herein.

c. The Authorized User has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Supplier's Cloud tenants for similar Cloud Services. Supplier's right to a new use agreement for new version releases of the Cloud Services shall not be abridged by the foregoing. Supplier may, at no additional charge, modify the Cloud Services to improve operation and reliability or to meet legal requirements.

d. The technical and professional activities required for managing and maintaining the Cloud Services are the responsibilities of the Supplier.

e. Cloud Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickthrough or shrinkwrap agreement. The term clickthrough or shrinkwrap agreement refers to passive consent based on terms either included at install or first use, an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Cloud Services. All terms and conditions of any clickthrough or shrinkwrap agreement provided with any Cloud Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.

f. Additional Cloud Services Terms.

(i) The State Entity shall: (1) be solely responsible for the accuracy, quality, integrity and legality of State Data; (2) prevent unauthorized use of the Cloud Services, and notify Supplier promptly of any such unauthorized use; (3) use the Cloud Services in accordance with the policies, descriptive content, and applicable Laws; (4) obtain any and all third-party consents necessary for the use and processing of State Data in connection with the Cloud Services; and (5) use the Cloud Services with only appropriately licensed and Supplier approved third party software and technology.

(ii) The State Entity shall not: (1) use the Cloud Services to store or transmit infringing, libelous, harmful or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights; (2) use the Cloud Services to store or transmit malicious code; (3) interfere with or disrupt the integrity or performance of the Cloud Services or related third-party data ; and (4) permit any third party to access the Cloud Services except the state Entity’s contractors.

(ii) ACCESS AVAILABILITY; REMEDIES:

a. The Supplier warrants that the Cloud Services will be in good working order and operate in conformance with Supplier's standard specifications and functions as

well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA.

(iii) MODIFICATION OF SERVICES: If Supplier modifies or replaces the Cloud Services, and if the State has paid all applicable Subscription Fees, the Authorized User shall be entitled to receive, at no additional charge, access to a newer version of the Cloud Services that supports the same functionality as the then accessible version of the Cloud Services. Newer versions of the Cloud Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Cloud Services shall remain fully available to the Authorized User until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Cloud Services as used by the State, the State, at its sole option, may defer such modification.

D. COMPENSATION

1. **Pricing and Payment.** The Supplier will be paid for the goods and services sold pursuant to the Statewide Contract in accordance with the RFX and final pricing documents as incorporated into the Statewide Contract Form and the terms of the Statewide Contract. Unless clearly stated otherwise in the Statewide Contract, all prices are firm and fixed and are not subject to variation. Prices include, but are not limited to freight, insurance, fuel surcharges and customs duties. User Agencies are solely and individually financially responsible for their respective purchases.

2. **Billings.** If applicable, and unless the RFX provides otherwise, the Supplier shall submit, on a regular basis, an invoice for goods and services supplied to the User Agencies under the Statewide Contract at the billing address specified in the Purchase Instrument or Statewide Contract. The invoice shall comply with all applicable rules concerning payment of such claims. User Agencies shall pay all approved invoices in arrears and in accordance with applicable provisions of State law.

   Unless otherwise agreed in writing by the Agency and the Supplier, the Supplier shall not be entitled to receive any other payment or compensation from the User Agencies for any goods or services provided by or on behalf of the Supplier under the Statewide Contract. The Supplier shall be solely responsible for paying all costs, expenses, and charges it incurs in connection with its performance under the Statewide Contract.

3. **Delay of Payment Due to Supplier's Failure.** If the User Agencies in good faith determine that the Supplier has failed to perform or deliver any service or product as required by the Statewide Contract, the Supplier shall not be entitled to any compensation under the Statewide Contract until such service or product is performed or delivered. In this event, the User Agencies may withhold that portion of the Supplier's compensation which represents payment for services or products that were not performed or delivered. To the extent that the Supplier's failure to perform or deliver in a timely manner causes the User Agencies to incur costs, the User Agencies may deduct the amount of such incurred costs from any amounts payable to Supplier. The User Agencies' authority to deduct such incurred costs shall not in any way affect the Agency's sole authority to terminate the Statewide Contract.

4. **Set-Off Against Sums Owed by the Supplier.** In the event that the Supplier owes the User Agency any sum or the User Agency must obtain substitute performance, the User Agency may set off the sum owed against any sum owed by the User Agency to the Supplier.

5. **Payment Disputes.** If Supplier disputes any calculation, determination or amount of any payment, Supplier shall notify the User Agency issuing the Order in writing of its dispute within 30 days following the earlier to occur of Supplier's receipt of the payment or notification of the determination or calculation of the payment by that User Agency. The User Agency will review the information presented by Supplier and may make changes to its determination based on this review. The calculation, determination, or payment amount that results from the User Agency's review shall not be subject to additional dispute under this subsection. No payment subject to a dispute under this subsection shall be due until after the User Agency has concluded its review, and the User Agency shall not pay any interest on any amount during the period it is subject to dispute under this subsection.

E. TERMINATION

1. **Immediate Termination.** Pursuant to O.C.G.A. Section 50-5-64, any purchase made pursuant to this Statewide Contract will terminate immediately and absolutely if the User Agency determines that adequate funds are not appropriated or granted or funds are de-appropriated such that the User Agency cannot fulfill its obligations under the Statewide Contract, which determination is at the User Agency's sole discretion and shall be conclusive. Further, the Agency may terminate the Statewide Contract for any one or more of the following reasons effective immediately without advance notice:

   (i) In the event the Supplier is required to be certified or licensed as a condition precedent to providing goods and services, the revocation or loss of such license or certification may result in immediate termination of the Statewide Contract effective as of the date on which the license or certification is no longer in effect;

   (ii) The Agency determines that the actions, or failure to act, of the Supplier, its agents, employees, or subcontractors have caused, or reasonably could cause, life, health, or safety to be jeopardized;

   (iii) The Supplier fails to comply with confidentiality laws or provisions; and/or

   (iv) The Supplier furnished any statement, representation, or certification in connection with the Statewide Contract or the bidding process, which is materially false, deceptive, incorrect, or incomplete.

2. **Termination for Cause.** The occurrence of any one or more of the following events shall constitute cause for the Agency to declare the Supplier in default of its obligations under the Statewide Contract:

   (i) The Supplier fails to deliver or has delivered nonconforming goods or services or fails to perform, to the Agency's satisfaction, any material requirement of the Statewide Contract or is in violation of a material provision of the Statewide Contract, including, but without limitation, the express warranties made by the Supplier;

   (ii) The Agency determines that satisfactory performance of the Statewide Contract is substantially endangered or that a default is likely to occur;

   (iii) The Supplier fails to make substantial and timely progress toward performance of the Statewide Contract;

(iv) The Supplier becomes subject to any bankruptcy or insolvency proceeding under federal or state law to the extent allowed by applicable federal or state law including bankruptcy laws; the Supplier terminates or suspends its business; or the Agency reasonably believes that the Supplier has become insolvent or unable to pay its obligations as they accrue consistent with applicable federal or state law;

(v) The Supplier has failed to comply with applicable federal, state, and local laws, rules, ordinances, regulations, and orders when performing within the scope of the Statewide Contract;

(vi) The Supplier has engaged in conduct that has or may expose the Agency or the State to liability, as determined in the Agency's sole discretion; or

(vii) The Supplier has infringed any patent, trademark, copyright, trade dress or any other intellectual property rights of the Agency, the State, or a third party.

3. Notice of Default. If there is a default event caused by the Supplier, the Agency shall provide written notice to the Supplier requesting that the breach or noncompliance be remedied within the period of time specified in the Agency's written notice to the Supplier. If the breach or noncompliance is not remedied within the period of time specified in the written notice, the Agency may:

(i) Immediately terminate the Statewide Contract without additional written notice; and/or

(ii) Procure substitute goods or services from another source and charge the difference between the Statewide Contract and the substitute contract to the defaulting Supplier; and/or,

(iii) Enforce the terms and conditions of the Statewide Contract and seek any legal or equitable remedies.

4. Termination Upon Notice. Following thirty (30) days' written notice, the Agency may terminate the Statewide Contract in whole or in part without the payment of any penalty or incurring any further obligation to the Supplier. Following termination upon notice, the Supplier shall be entitled to compensation from the User Agency, upon submission of invoices and proper proof of claim, for goods and services provided under the Statewide Contract to the User Agencies up to and including the date of termination.

5. Termination Due to Change in Law. The Agency shall have the right to terminate this Statewide Contract without penalty by giving thirty (30) days' written notice to the Supplier as a result of any of the following:

(i) The Agency's authorization to operate is withdrawn or there is a material alteration in the programs administered by the Agency; and/or

(ii) The Agency's duties are substantially modified.

6. Payment Limitation in Event of Termination. In the event of termination of the Statewide Contract for any reason by the Agency, the User Agencies shall pay only those amounts, if any, due and owing to the Supplier for goods and services actually rendered up to the date specified in the notice of termination for which the User Agencies are obligated to pay pursuant to the Statewide Contract or Purchase Instrument. Payment will be made only upon submission of invoices and proper proof of the Supplier's claim. This provision in no way limits the remedies

available to the State under the Statewide Contract in the event of termination. The State shall not be liable for any costs incurred by the Supplier in its performance of the Statewide Contract, including, but not limited to, startup costs, overhead or other costs associated with the performance of the Statewide Contract.

7. **The Supplier's Termination Duties.** Upon receipt of notice of termination or upon request of the Agency, the Supplier shall:

   (i) Cease work under the Statewide Contract and take all necessary or appropriate steps to limit disbursements and minimize costs, and furnish a report within thirty (30) days of the date of notice of termination, describing the status of all work under the Statewide Contract, including, without limitation, results accomplished, conclusions resulting therefrom, and any other matters the Agency may require;

   (ii) Immediately cease using and return to the State, any personal property or materials, whether tangible or intangible, provided by the State to the Supplier;

   (iii) Comply with the State's instructions for the timely transfer of any active files and work product produced by the Supplier under the Statewide Contract;

   (iv) Cooperate in good faith with the Agency, the User Agencies, and their employees, agents, and Suppliers during the transition period between the notification of termination and the substitution of any replacement Supplier; and

   (v) Immediately return to the User Agencies any payments made by the User Agencies for goods and services that were not delivered or rendered by the Supplier.

   (vi) Orders may only be placed prior to the expiration or earlier termination of this Contract but may have a delivery date or performance period that extends after the expiration or earlier termination date. Regardless of whether this Contract has expired or has been terminated, the Supplier shall comply with all Orders that extend past the expiration or termination, as described in this section, and all requirements of this Contract necessary to complete outstanding Orders shall survive the expiration or termination of this Contract until all Orders are complete. Any Orders submitted prior to the expiration or termination of this Contract shall be governed by the terms and conditions of this Contract.

F. CONFIDENTIAL INFORMATION

1. **Access to Confidential Data.** The Supplier's employees, agents and subcontractors may have access to confidential data maintained by the State to the extent necessary to carry out the Supplier's responsibilities under the Statewide Contract. The Supplier shall presume that all information received pursuant to the Statewide Contract is confidential unless otherwise designated by the State. If it is reasonably likely the Supplier will have access to the State's confidential information, then:

   (i) The Supplier shall provide to the State a written description of the Supplier's policies and procedures to safeguard confidential information;

   (ii) Policies of confidentiality shall address, as appropriate, information conveyed in verbal, written, and electronic formats;

(iii) The Supplier must designate one individual who shall remain the responsible authority in charge of all data collected, used, or disseminated by the Supplier in connection with the performance of the Statewide Contract; and

(iv) The Supplier shall provide adequate supervision and training to its agents, employees, and subcontractors to ensure compliance with the terms of the Statewide Contract.

The private or confidential data shall remain the property of the State at all times. Some services performed for the Agency and/or User Agencies may require the Supplier to sign a nondisclosure agreement. Supplier understands and agrees that refusal or failure to sign such a nondisclosure agreement, if required, may result in termination of the Statewide Contract.

2. **No Dissemination of Confidential Data.** No confidential data collected, maintained, or used in the course of performance of the Statewide Contract shall be disseminated except as authorized by law and with the written consent of the State, either during the period of the Statewide Contract or thereafter. Any data supplied to or created by the Supplier shall be considered the property of the State. The Supplier must return any and all data collected, maintained, created, or used in the course of the performance of the Statewide Contract, in whatever form it is maintained, promptly at the request of the State.

3. **Subpoena.** In the event that a subpoena or other legal process is served upon the Supplier for records containing confidential information, the Supplier shall promptly notify the State and cooperate with the State in any lawful effort to protect the confidential information.

4. **Reporting of Unauthorized Disclosure.** The Supplier shall immediately report to the State any unauthorized disclosure of confidential information.

5. **Survives Termination.** The Supplier's confidentiality obligation under the Statewide Contract shall survive termination of the Statewide Contract.

G. INDEMNIFICATION

1. **Supplier's Indemnification Obligation.** The Supplier agrees to indemnify and hold harmless the State and State officers, employees, agents, and volunteers (collectively, "Indemnified Parties") from any and all costs, expenses, losses, claims, damages, liabilities, settlements, and judgments, including reasonable value of the time spent by the Attorney General's Office, related to, or arising from a third-party claim for:

(i) Any breach of the Statewide Contract;

(ii) Any negligent, intentional, or wrongful act or omission of the Supplier or any employee, agent or subcontractor utilized or employed by the Supplier;

(iii) Any failure of goods to comply with applicable specifications, warranties, and certifications under the Statewide Contract;

(iv) The negligence or fault of the Supplier in design, testing, development, manufacture, or otherwise with respect to the goods or any parts thereof provided under the Statewide Contract;

(v) Claims, demands, or lawsuits that, with respect to the goods or any parts thereof, allege product liability, strict product liability, or any variation thereof;

(vi) Any failure by the Supplier to comply with the "Compliance with the Law" provision of the Statewide Contract;

(vii) Any failure by the Supplier to make all reports, payments and withholdings required by federal and state law with respect to social security, employee income and other taxes, fees or costs required by the Supplier to conduct business in the State of Georgia or the United States;

(viii) Any infringement of any copyright, trademark, patent, trade dress, or other intellectual property right; or

(ix) Any failure by the Supplier to adhere to the confidentiality provisions of the Statewide Contract.

2. **Duty to Reimburse State Tort Claims Fund.** To the extent such damage or loss as covered by this indemnification is covered by the State of Georgia Tort Claims Fund ("the Fund"), the Supplier (and its insurers) agrees to reimburse the Fund. To the full extent permitted by the Constitution and the laws of the State and the terms of the Fund, the Supplier and its insurers waive any right of subrogation against the State, the Indemnified Parties, and the Fund and insurers participating thereunder, to the full extent of this indemnification.

3. **Litigation and Settlements.** The Supplier shall, at its own expense, be entitled to and shall have the duty to participate in the defense of any suit against the Indemnified Parties. No settlement or compromise of any claim, loss or damage entered into by the Indemnified Parties shall be binding upon Supplier unless approved in writing by Supplier. No settlement or compromise of any claim, loss or damage entered into by Supplier shall be binding upon the Indemnified Parties unless approved in writing by the Indemnified Parties.

4. **Patent/Copyright Infringement Indemnification.** Supplier shall, at its own expense, be entitled to and shall have the duty to participate in the defense of any suit instituted against the State and indemnify the State against any award of damages and costs made against the State by a final judgment of a court of last resort in such suit insofar as the same is based on any claim that any of the software constitutes an infringement of any United States Letters Patent or copyright, provided the State gives the Supplier immediate notice in writing of the institution of such suit, permits Supplier to fully participate in the defense of the same, and gives Supplier all available information, assistance and authority to enable Supplier to do so. Subject to approval of the Attorney General of the State of Georgia, the Agency shall tender defense of any such action to Supplier upon request by Supplier. Supplier shall not be liable for any award of judgment against the State reached by compromise or settlement unless Supplier accepts the compromise or settlement. Supplier shall have the right to enter into negotiations for and the right to effect settlement or compromise of any such action, but no such settlement shall be binding upon the State unless approved by the State.

   In case any of the software is in any suit held to constitute infringement and its use is enjoined, Supplier shall, at its option and expense:

   (i) Procure for the State the right to continue using the software;

   (ii) Replace or modify the same so that it becomes non-infringing; or

   (iii) Remove the same and cancel any future charges pertaining thereto.

Supplier, however, shall have no liability to the State if any such patent, or copyright infringement or claim thereof is based upon or arises out of:

(i) Compliance with designs, plans or specifications furnished by or on behalf of the Agency as to the software;

(ii) Use of the software in combination with apparatus or devices not supplied by Supplier;

(iii) Use of the software in a manner for which the same was neither designed nor contemplated; or

(iv) The claimed infringement of any patent or copyright in which the Agency or any affiliate or subsidiary of the Agency has any direct interest by license or otherwise.

5. Survives Termination. The indemnification obligation of the Supplier shall survive termination of the Statewide Contract.

H. INSURANCE

Within ten (10) business days of award and before commencing work on this Contract, Supplier must provide USER AGENCY with certificates of insurance to show that the following minimum coverages are in effect. It is the responsibility of Supplier to maintain current certificates of insurance on file with the State through the term of this Agreement. No warranty is made that the coverages and limits listed herein are adequate to cover and protect the interests of Supplier for Supplier's operations. These are solely minimums that have been established to protect the interests of the State. Supplier shall procure and maintain the insurance policies described below and shall furnish USER AGENCY two insurance certificates referencing the contract number. The certificates must list the State of Georgia as certificate holder and as an additional insured on the Commercial General Liability policy. The insurance certificates must document that the Commercial General Liability insurance coverage provided by Supplier includes contractual liability coverage applicable to the Contract. In addition, the insurance certificate must provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company; a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions, and endorsements); and an acknowledgment of notice of cancellation to USER AGENCY. The State does not require Authorized Servicing Partners to maintain the insurance requirements described below, which are at the discretion of Supplier. Supplier is required to maintain the following insurance coverage's during the term of the Contract:

A. Workers Compensation Insurance (Occurrence) in the amounts of the statutory limits established by applicable law (A self-insurer must submit a certificate from the applicable state entity stating that Supplier qualifies to pay its own workers compensation claims.) In addition, Supplier shall require all subcontractors performing work under the Contract to obtain an insurance certificate showing proof of Workers Compensation Coverage with the following minimum coverage:

Bodily injury by accident - per employee	$100,000;
Bodily injury by disease - per employee	$100,000;
Bodily injury by disease – policy limit	$500,000.

B. Commercial General Liability Policy with the following minimum coverage:

Each Occurrence Limit	$1,000,000
Personal & Advertising Injury Limit	$1,000,000
General Aggregate Limit	$2,000,000
Products/Completed Ops. Aggregate Limit	$2,000,000

C. Technical Errors and Omissions and Privacy, Cyber Security and Technology which shall include third party liability coverages, including network security/privacy coverage and technology errors and omissions coverage.

Technical Errors and Omissions and Privacy Policy shall include:

1. Technology Errors and Omissions
2. Multimedia Liability
3. Privacy Liability
4. Network Security Liability
5. Breach Costs Coverage – Notification, Credit Monitoring, Forensics, Public Relations
6. Regulatory Fines and Penalties assessed due to a Data (Privacy) Breach

Privacy, Security and Technology Policy shall include:

1. Coverage for loss, disclosure, and theft of data in any form
2. Multimedia Liability
3. Software copyright infringement
4. Network Security Liability
5. Breach Costs Coverage – Notification, Credit Monitoring, Forensics, Public Relations
6. Regulatory Fines and Penalties assessed due to a Data (Privacy) Breach

Per Occurrence/Aggregate Limit $15,000,000.

D. Umbrella Liability $2,000,000

E. Automobile Liability

Combined Single Limit	$1,000,000

Additional Insurance Requirements

Should any of the foregoing policies be cancelled before the expiration date thereof, notice will be delivered in accordance with the policy provisions. In addition, Supplier shall notify the State immediately upon receiving any information that any of the coverages required herein are or will be changed, cancelled, or replaced. The foregoing policies shall be obtained from insurance companies licensed or authorized to do business in Georgia and shall be with companies acceptable to DOAS, which must have a minimum A.M. Best rating of A-. All such coverage shall remain in full force and effect during the term and any renewal or extension thereof.

I. BONDS

The Supplier shall provide all required bonds in accordance with the terms of the RFX and as stated in the Statewide Contract Form.

J. WARRANTIES

1. **Construction of Warranties Expressed in the Contract with Warranties Implied by Law.** All warranties made by the Supplier and/or subcontractor in all provisions of the Statewide Contract and the Supplier's Response, whether or not the Statewide Contract specifically denominates the Supplier's and/or subcontractor's promise as a warranty or whether the warranty is created only by the Supplier's affirmation or promise, or is created by a description of the materials, goods and services to be provided, or by provision of samples to the State shall not be construed as limiting or negating any warranty provided by law, including without limitation, warranties which arise through course of dealing or usage of trade, the warranty of merchantability, and the warranty of fitness for a particular purpose. The warranties expressed in the Statewide Contract are intended to modify the warranties implied by law only to the extent that they expand the warranties applicable to the goods and services provided by the Supplier. The provisions of this section apply during the term of the Statewide Contract and any extensions or renewals thereof.

2. **Warranty – Nonconforming Goods.** All goods delivered by Supplier to the User Agencies shall be free from any defects in design, material, or workmanship. If any goods offered by the Supplier are found to be defective in material or workmanship, or do not conform to Supplier's warranty, the User Agencies shall have the option of returning, repairing, or replacing the defective goods at Supplier's expense. Payment for goods shall not constitute acceptance. Acceptance by the User Agencies shall not relieve the Supplier of its warranty or any other obligation under the Statewide Contract.

3. **Compliance with Federal Safety Acts.** Supplier warrants and guarantees to the State that the goods provided under the Statewide Contract are in compliance with Sections 5 and 12 of the Federal Trade Commission Act; the Fair Packaging and Labeling Act; the Federal Food, Drug, and Cosmetic Act; the Consumer Product Safety Act; the Federal Environmental Pesticide Control Act; the Federal Hazardous Substances Act; the Fair Labor Standards Act; the Wool Products Labeling Act; the Flammable Fabrics Act; the Occupational Safety and Health Act; the Office of Management and Budget A-110 Appendix A; and the Anti-Kickback Act of 1986.

4. **Originality and Title to Concepts, Materials, and Goods Produced.** Supplier represents and warrants that all the concepts, materials, goods, and services produced, or provided to the State pursuant to the terms of the Statewide Contract shall be wholly original with the Supplier or that the Supplier has secured all applicable interests, rights, licenses, permits or other intellectual property rights in such concepts, materials and works. The Supplier represents and warrants that the concepts, materials, goods and services and the State's use of same and the exercise

by the State of the rights granted by the Statewide Contract shall not infringe upon any other work, other than material provided by the Statewide Contract to the Supplier to be used as a basis for such materials, or violate the rights of publicity or privacy of, or constitute a libel or slander against, any person, firm or corporation and that the concepts, materials and works will not infringe upon the copyright, trademark, trade name, trade dress patent, literary, dramatic, statutory, common law or any other rights of any person, firm or corporation or other entity. The Supplier represents and warrants that it is the owner of or otherwise has the right to use and distribute the goods and services contemplated by the Statewide Contract.

5. **Conformity with Contractual Requirements.** The Supplier represents and warrants that the goods and services provided in accordance with the Statewide Contract will appear and operate in conformance with the terms and conditions of the Statewide Contract.

6. **Authority to Enter into Contract.** The Supplier represents and warrants that it has full authority to enter into the Statewide Contract and that it has not granted and will not grant any right or interest to any person or entity that might derogate, encumber, or interfere with the rights granted to the State.

7. **Obligations Owed to Third Parties.** The Supplier represents and warrants that all obligations owed to third parties with respect to the activities contemplated to be undertaken by the Supplier pursuant to the Statewide Contract are or will be fully satisfied by the Supplier so that the State will not have any obligations with respect thereto.

8. **Title to Property.** The Supplier represents and warrants that title to any property assigned, conveyed, or licensed to the State is good and that transfer of title or license to the State is rightful and that all property shall be delivered free of any security interest or other lien or encumbrance. Title to any supplies, materials, or equipment shall remain in the Supplier until fully paid for by the User Agencies.

9. **Industry Standards.** The Supplier represents and expressly warrants that all aspects of the goods and services provided or used by it shall at a minimum conform to the standards in the Supplier's industry. This requirement shall be in addition to any express warranties, representations, and specifications included in the Statewide Contract, which shall take precedence.

10. Supplier's Personnel and Staffing.

(i) Staffing Assignments and Credentials

a. Supplier warrants and represents that all persons, including independent Suppliers and consultants assigned by it to the performance of this Contract, shall be employees or formal agents of Supplier and shall have the credentials necessary (i.e., licensed, and bonded, as required) to perform the work required herein; failure to notify User Agency of replacement of subcontractors or staff assigned to perform the work will be considered breach of contract. Supplier shall include a similar provision in any contract with any subcontractor selected to perform work hereunder. Supplier also agrees that User Agency may approve or disapprove Supplier's subcontractors, or its staff assigned to provide services prior to the proposed staff assignment or change in staffing. The State shall have the right at any time to require the Supplier remove from interaction with State any Supplier representative who the State believes is detrimental to its working relationship with the Supplier. The State shall provide the Supplier with notice of its determination,

and the reasons it requests the removal. The Supplier shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

b. In addition, Supplier warrants that all persons it assigns to perform work under this Contract shall be employees or authorized subcontractors of Supplier and shall be fully qualified to perform the services required herein. Personnel commitments shall not be changed unless approved by User Agency in writing. Staffing will include the named individuals at the levels of effort specified in the Statement of Work.

c. Supplier shall provide and maintain sufficient qualified personnel and staffing to enable the deliverables to be provided in accordance with the Statement of Work. Supplier also warrants that it will comply with all other staffing/personnel obligations set out herein, including but not limited to those pertaining to security, health, and safety issues.

d. Supplier warrants that all staff performing services pursuant to this Contract shall be located entirely within the boundaries of the United States and that no staff (including but not limited to subcontractors) used in the performance of this Contract shall perform services from an Offshore location unless approved by the User Agency in compliance with the policies standards and guidelines of the Georgia Technology Authority (GTA). Such approval is within User Agency's sole discretion.

(ii) Staffing Changes

a. User Agency may reject any proposed changes in Key Staff or require the removal or reassignment of any Supplier employee or subcontractor employee that User Agency deems to be unacceptable. User Agency's decision on this matter shall be final, subject to the Dispute Resolution provisions.

b. Notwithstanding the above provisions, the Parties acknowledge and agree that the Supplier may terminate any of its employees designated to perform work or services under this Contract, as permitted by applicable law. In the event Supplier terminates one of its employees that performs services under this Contract, Supplier will provide User Agency with immediate notice of the termination and an action plan for replacing the discharged employee with a person of at least equivalent training, experience, and talent within (2) calendar days of the termination. The Parties understand that time is of the essence and Supplier will immediately fill any vacated role temporarily until the permanent replacement can be filled consistent with these terms provided herein.

11. Use of State Vehicles. Supplier warrants that no State vehicles will be used by Supplier for the performance of services under this Statewide Contract. Supplier shall be responsible for providing transportation necessary to perform all services.

12. Responsibility. Supplier represents and warrants that it shall remain responsible at all times during the term of the Contract, maintaining legal authority to do business in the State of Georgia, a satisfactory record of integrity, appropriate financial, organizational, and operational capacity and control, and acceptable performance on previous and current governmental and/or private contracts, if any.

13. Workmanship warranty period.
For all networking installed projects, systems, and all related services, Suppliers must guarantee a workmanship warranty period of one hundred and eighty (180) days from Acceptance of the deliverable, or such longer period as may be agreed to in the applicable SOW.

13. Web Accessibility. As applicable to the services being provided under the Contract, Supplier warrants that:

(i) Its products and services comply with and shall remain in compliance with all applicable federal disability laws and regulations, including but not limited to the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended, and its implementing regulations; and

(ii) Its products and services, as applicable, conform with the prevailing Web Content Accessibility Guidelines (WCAG) Standards to AA level-currently WCAG 2.1 AA;

(iii) Supplier shall maintain, retain, and provide to the State upon request its accessibility testing results and written documentation verifying accessibility in a Voluntary Product Accessibility Template (VPAT) or other format specified by the State;

(iv) It shall permit the state to conduct an accessibility audit by any auditor of the State's choice and promptly respond to, resolve, and remediate at no cost to the state any complaint regarding accessibility of its products and services; and

(v) It shall hold the State harmless from and indemnify the State for any claims arising out of its failure to comply with these obligations.

K. PRODUCT RECALL

In the event that any of the goods are found by the Supplier, the State, any governmental agency, or court having jurisdiction to contain a defect, serious quality or performance deficiency, or not to be in compliance with any standard or requirement so as to require or make advisable that such goods be reworked or recalled, the Supplier will promptly communicate all relevant facts to the Agency and undertake all corrective actions, including those required to meet all obligations imposed by laws, regulations, or orders, and shall file all necessary papers, corrective action programs, and other related documents, provided that nothing contained in this section shall preclude the Agency from taking such action as may be required of it under any such law or regulation. The Supplier shall perform all necessary repairs or modifications at its sole expense except to any extent that the Supplier and the State shall agree to the performance of such repairs by the State upon mutually acceptable terms.

L. CONTRACT ADMINISTRATION

1. Order of Preference. In the case of any inconsistency or conflict among the specific provisions of the Statewide Contract Terms and Conditions (including any amendments accepted by both the Agency and the Supplier attached hereto and the Awarded Item Schedule, if any), the RFX (including any subsequent addenda and written responses to bidders' questions), and the Supplier's Response, any inconsistency or conflict shall be resolved as follows:

(i) First, by giving preference to the Statewide Contract Terms and Conditions.

(ii) Second, by giving preference to the specific provisions of the RFX.

(iii) Third, by giving preference to the specific provisions of the Supplier's Response, except that objections or amendments by a Supplier that have not been explicitly accepted by the Agency in writing shall not be included in this Statewide Contract and shall be given no weight or consideration.

(iv) State of Georgia, DOAS, Data Security Terms & Conditions.

(v) JUNIPER PURCHASE AND LICENSE AGREEMENT as modified by the parties and attached.

2. **Intent of References to Bid Documents.** The references to the parties' obligations, which are contained in this document, are intended to supplement, or clarify the obligations as stated in the RFX and the Supplier's Response. The failure of the parties to make reference to the terms of the RFX or the Supplier's Response in this document shall not be construed as creating a conflict and will not relieve the Supplier of the contractual obligations imposed by the terms of the RFX and the Supplier's Response. The contractual obligations of the Agency cannot be implied from the Supplier's Response.

3. **Compliance with the Law.** The Supplier, its employees, agents, and subcontractors shall comply with all applicable federal, state, and local laws, rules, ordinances, regulations, and orders now or hereafter in effect when performing under the Statewide Contract, including without limitation, all laws applicable to the prevention of discrimination in employment and the use of targeted small businesses as subcontractors or Suppliers. The Supplier, its employees, agents, and subcontractors shall also comply with all federal, state, and local laws regarding business permits and licenses that may be required to carry out the work performed under the Statewide Contract. Supplier and Supplier's personnel shall also comply with all State, Agency, and User Agency policies and standards in effect during the performance of the Statewide Contract, including but not limited to the Agency and User Agencies' policies and standards relating to personnel conduct, security, safety, confidentiality, and ethics. Further, the provisions of O.C.G.A. Section 45-10-20 et seq. have not and must not be violated under the terms of this Statewide Contract. If the value of this Contract is $100,000 or more and Supplier is a company that employs more than five persons, Supplier certifies that Supplier is not currently engaged in, and agrees for the duration of this Contract not to engage in, a boycott of Israel, as defined in O.C.G.A. §50-5-85.

4. **Drug-free Workplace.** The Supplier hereby certifies as follows:

(i) Supplier will not engage in the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana during the performance of this Statewide Contract; and

(ii) If Supplier has more than one employee, including Supplier, Supplier shall provide for such employee(s) a drug-free workplace, in accordance with the Georgia Drug-free Workplace Act as provided in O.C.G.A. Section 50-24-1 et seq., throughout the duration of this Statewide Contract; and

(iii) Supplier will secure from any subcontractors hired to work on any job assigned under this Statewide Contract the following written certification: "As part of the subcontracting agreement with (Supplier's Name), (subcontractor's Name) certifies to the Supplier that a drug-free workplace will be provided for the subcontractor's employees during the performance of this Contract pursuant to paragraph 7 of subsection (b) of Code Section 50-24-3."

Supplier may be suspended, terminated, or debarred if it is determined that:

(i) Supplier has made false certification here in above; or

(ii) Supplier has violated such certification by failure to carry out the requirements of O.C.G.A. Section 50-24-3(b).

5. Amendments. The Statewide Contract may be amended in writing from time to time by mutual consent of the parties and upon approval by the Agency. All amendments to the Statewide Contract must be in writing and fully executed by duly authorized representatives of the Agency and the Supplier.

6. Third Party Beneficiaries. There are no third-party beneficiaries to the Statewide Contract. The Statewide Contract is intended only to benefit the State and the Supplier.

7. Choice of Law and Forum. The laws of the State of Georgia shall govern and determine all matters arising out of or in connection with this Statewide Contract without regard to the choice of law provisions of State law. In the event any proceeding of a quasi-judicial or judicial nature is commenced in connection with this Statewide Contract, such proceeding shall solely be brought in a court or other forum of competent jurisdiction within Fulton County, Georgia. This provision shall not be construed as waiving any immunity to suit or liability, including without limitation sovereign immunity, which may be available to the State.

8. Parties' Duty to Provide Notice of Intent to Litigate and Right to Demand Mediation. In addition to any dispute resolution procedures otherwise required under this Statewide Contract or any informal negotiations which may occur between the State and the Supplier, no civil action with respect to any dispute, claim or controversy arising out of or relating to this Statewide Contract may be commenced without first giving fourteen (14) calendar days written notice to the State of the claim and the intent to initiate a civil action. At any time prior to the commencement of a civil action, either the State or the Supplier may elect to submit the matter for mediation. Either the State or the Supplier may exercise the right to submit the matter for mediation by providing the other party with a written demand for mediation setting forth the subject of the dispute. The parties will cooperate with one another in selecting a mediator and in scheduling the mediation proceedings. Venue for the mediation will be in Atlanta, Georgia; provided, however, that any or all mediation proceedings may be conducted by teleconference with the consent of the mediator. The parties covenant that they will participate in the mediation in good faith, and that they will share equally in its costs; provided, however that the cost to the State shall not exceed five thousand dollars ($5,000.00).

All offers, promises, conduct and statements, whether oral or written, made in the course of the mediation by any of the parties, their agents, employees, experts and attorneys, and by the mediator or employees of any mediation service, are inadmissible for any purpose (including but not limited to impeachment) in any litigation or other proceeding involving the parties, provided that evidence that is otherwise admissible or discoverable shall not be rendered inadmissible or non-discoverable as a result of its use in the mediation. Inadmissibility notwithstanding, all written documents shall nevertheless be subject to the Georgia Open Records Act O.C.G.A. Section 50-18-70 et.seq.

No party may commence a civil action with respect to the matters submitted to mediation until after the completion of the initial mediation session, forty-five (45) calendar days after the date of filing the written request for mediation with the mediator or mediation service, or sixty (60) calendar days after the delivery of the written demand for mediation, whichever occurs first. Mediation may continue after the commencement of a civil action if the parties so desire.

9. Assignment and Delegation. The Statewide Contract may not be assigned, transferred, or conveyed in whole or in part without the prior written consent of the Agency. For the purpose of

construing this clause, a transfer of a controlling interest in the Supplier shall be considered an assignment.

10. **Use of Third Parties.** Except as may be expressly agreed to in writing by the Agency, Supplier shall not subcontract, assign, delegate or otherwise permit anyone other than Supplier or Supplier's personnel to perform any of Supplier's obligations under this Statewide Contract or any of the work subsequently assigned under this Statewide Contract. No subcontract which Supplier enters into with respect to performance of obligations or work assigned under the Statewide Contract shall in any way relieve Supplier of any responsibility, obligation, or liability under this Statewide Contract and for the acts and omissions of all subcontractors, agents, and employees. All restrictions, obligations and responsibilities of the Supplier under the Statewide Contract shall also apply to the subcontractors. Any contract with a subcontractors must also preserve the rights of the Agency. The Agency shall have the right to request the removal of a subcontractors from the Statewide Contract for good cause.

11. **Integration.** The Statewide Contract represents the entire agreement between the parties. The parties shall not rely on any representation that may have been made which is not included in the Statewide Contract.

12. **Headings or Captions.** The paragraph headings or captions used in the Statewide Contract are for identification purposes only and do not limit or construe the contents of the paragraphs.

13. **Not a Joint Venture.** Nothing in the Statewide Contract shall be construed as creating or constituting the relationship of a partnership, joint venture, (or other association of any kind or agent and principal relationship) between the parties thereto. Each party shall be deemed to be an independent Supplier contracting for goods and services and acting toward the mutual benefits expected to be derived herefrom. Neither Supplier nor any of Supplier's agents, servants, employees, subcontractors, or Suppliers shall become or be deemed to become agents, servants, or employees of the State. Supplier shall therefore be responsible for compliance with all laws, rules and regulations involving its employees and any subcontractors, including but not limited to employment of labor, hours of labor, health, and safety, working conditions, workers' compensation insurance, and payment of wages. No party has the authority to enter into any contract or create an obligation or liability on behalf of, in the name of, or binding upon another party to the Statewide Contract.

14. **Joint and Several Liability.** If the Supplier is a joint entity, consisting of more than one individual, partnership, corporation, or other business organization, all such entities shall be jointly and severally liable for carrying out the activities and obligations of the Statewide Contract, and for any default of activities and obligations.

15. **Supersedes Former Contracts or Agreements.** Unless otherwise specified in the Statewide Contract, this Statewide Contract supersedes all prior contracts or agreements between the Agency and the Supplier for the goods and services provided in connection with the Statewide Contract.

16. **Waiver.** Except as specifically provided for in a waiver signed by duly authorized representatives of the Agency and the Supplier, failure by either party at any time to require performance by the other party or to claim a breach of any provision of the Statewide Contract shall not be construed as affecting any subsequent right to require performance or to claim a breach.

17. **Notice.** Any and all notices, designations, consents, offers, acceptances or any other communication provided for herein shall be given in writing by registered or certified mail, return

receipt requested, by receipted hand delivery, by Federal Express, courier or other similar and reliable carrier which shall be addressed to the person who signed the Statewide Contract on behalf of the party at the address identified in the Statewide Contract Form. Each such notice shall be deemed to have been provided:

(i) At the time it is actually received; or,

(ii) Within one (1) day in the case of overnight hand delivery, courier, or services such as Federal Express with guaranteed next day delivery; or,

(iii) Upon receipt or refusal to accept delivery after it is deposited in the U.S. Mail in the case of certified or registered U.S. Mail.

From time to time, the parties may change the name and address of the person designated to receive notice. Such change of the designated person shall be in writing to the other party and as provided herein.

18. Cumulative Rights. The various rights, powers, options, elections and remedies of any party provided in the Statewide Contract shall be construed as cumulative and not one of them is exclusive of the others or exclusive of any rights, remedies or priorities allowed either party by law, and shall in no way affect or impair the right of any party to pursue any other equitable or legal remedy to which any party may be entitled as long as any default remains in any way unremedied, unsatisfied or undischarged.

19. Severability. If any provision of the Statewide Contract is determined by a court of competent jurisdiction to be invalid or unenforceable, such determination shall not affect the validity or enforceability of any other part or provision of the Statewide Contract. Further, if any provision of the Statewide Contract is determined to be unenforceable by virtue of its scope but may be made enforceable by a limitation of the provision, the provision shall be deemed to be amended to the minimum extent necessary to render it enforceable under the applicable law. Any agreement of the Agency and the Supplier to amend, modify, eliminate, or otherwise change any part of this Statewide Contract shall not affect any other part of this Statewide Contract, and the remainder of this Statewide Contract shall continue to be of full force and effect.

20. Time is of the Essence. Time is of the essence with respect to the performance of the terms of the Statewide Contract. Supplier shall ensure that all personnel providing goods and services to the State are responsive to the State's requirements and requests in all respects.

21. Authorization. The persons signing this Statewide Contract represent and warrant to the other parties that:

(i) It has the right, power, and authority to enter into and perform its obligations under the Statewide Contract; and

(ii) It has taken all requisite action (corporate, statutory, or otherwise) to approve execution, delivery and performance of the Statewide Contract and the Statewide Contract constitutes a legal, valid, and binding obligation upon itself in accordance with its terms.

22. Successors in Interest. All the terms, provisions, and conditions of the Statewide Contract shall be binding upon and inure to the benefit of the parties hereto and their respective successors, assigns and legal representatives.

23. **Record Retention and Access.** The Supplier shall maintain books, records, and documents which sufficiently and properly document and calculate all charges billed to the State throughout the term of the Statewide Contract for a period of at least five (5) years following the date of final payment or completion of any required audit, whichever is later. The Supplier should maintain separate accounts and records for the Agency and the User Agencies. Records to be maintained include both financial records and service records. The Supplier shall permit the Auditor of the State of Georgia or any authorized representative of the State, and where federal funds are involved, the Comptroller General of the United States, or any other authorized representative of the United States government, to access and examine, audit, excerpt and transcribe any directly pertinent books, documents, papers, electronic or optically stored and created records or other records of the Supplier relating to orders, invoices or payments or any other documentation or materials pertaining to the Statewide Contract, wherever such records may be located during normal business hours. The Supplier shall not impose a charge for audit or examination of the Supplier's books and records. If an audit discloses incorrect billings or improprieties, the State reserves the right to charge the Supplier for the cost of the audit and appropriate reimbursement. Evidence of criminal conduct will be turned over to the proper authorities.

24. **Solicitation.** The Supplier warrants that no person or selling agency (except bona fide employees or selling agents maintained for the purpose of securing business) has been employed or retained to solicit and secure the Statewide Contract upon an agreement or understanding for commission, percentage, brokerage, or contingency.

25. **Public Records.** The laws of the State of Georgia, including the Georgia Open Records Act, as provided in O.C.G.A. Section 50-18-70 et seq., require procurement records and other records to be made public unless otherwise provided by law.

26. **Clean Air and Water Certification.** Supplier certifies that none of the facilities it uses to produce goods provided under the Statewide Contract are on the Environmental Protection Agency (EPA) List of Violating Facilities. Supplier will immediately notify the Agency of the receipt of any communication indicating that any of Supplier's facilities are under consideration to be listed on the EPA List of Violating Facilities.

27. **Debarred, Suspended, and Ineligible Status.** Supplier certifies that the Supplier and/or any of its subcontractors have not been debarred, suspended, or declared ineligible by any agency of the State of Georgia or as defined in the Federal Acquisition Regulation (FAR) 48 C.F.R. Ch.1 Subpart 9.4. Supplier will immediately notify the Agency if Supplier is debarred by the State or placed on the Consolidated List of Debarred, Suspended, and Ineligible Suppliers by a federal entity.

28. **Use of Name or Intellectual Property**. Supplier agrees it will not use the name or any intellectual property, including but not limited to, State trademarks or logos in any manner, including commercial advertising or as a business reference, without the expressed prior written consent of the State.

29. **Taxes.** User Agencies are exempt from Federal Excise Taxes, and no payment will be made for any taxes levied on Supplier's employee's wages. User Agencies are exempt from State and Local Sales and Use Taxes on the services. Tax Exemption Certificates will be furnished upon request. Supplier or an authorized subcontractor has provided the Agency with a sworn verification regarding the filing of unemployment taxes or persons assigned by Supplier to perform services required in this Statewide Contract, which verification is incorporated herein by reference.

30. **Certification Regarding Sales and Use Tax.** By executing the Statewide Contract, the Supplier certifies it is either (a) registered with the State Department of Revenue, collects, and remits State sales and use taxes as required by Georgia law, including Chapter 8 of Title 48 of the O.C.G.A.; or (b) not a "retailer" as defined in O.C.G.A. Section 48-8-2. The Supplier also acknowledges that the State may declare the Statewide Contract void if the above certification is false. The Supplier also understands that fraudulent certification may result in the Agency or its representative filing for damages for breach of contract.

31. **Delay or Impossibility of Performance.** Neither party shall be in default under the Contract if performance is delayed or made impossible by circumstances beyond such party's reasonable control and without such party's fault or negligence, including, but not limited to, an act of God, natural disaster, extreme weather, war, terrorist attack, riot, embargo, governmental order or declaration of emergency, quarantine, epidemic, pandemic, or public health emergency. In each such case, the delay or impossibility must be beyond the control and without the fault or negligence of the Supplier. If delay results from a subcontractor's conduct, negligence, or failure to perform, the Supplier shall not be excused from compliance with the terms and obligations of the Contract.

32. **Limitation of Contractor's Liability to the State.** Except as otherwise provided in this Contract, Supplier's liability to the State for any claim of damages arising out of this Contract shall be limited to direct damages and shall not exceed two times the total amount payable to Supplier over the duration of the Contract prior to the event or circumstances that first gave rise to such liability, or $5,000,000, whichever is the greatest.

    Notwithstanding the above, no limitation of Supplier's liability to the State shall apply to Supplier's liability for (a) claims for loss of or damage to real or tangible personal property;, (b) claims for personal injury or bodily injury, including death; (c) claims resulting from gross negligence, recklessness, bad faith, or intentional misconduct; (d) amounts due or obligations under a clause providing for liquidated damages or, if such clause is ruled unenforceable, as a penalty; (e) Supplier's indemnification obligations hereunder; (f) reserved; (g) breach of confidentiality obligations; or (h) any loss or claim to the extent such loss or claim is covered by a policy of insurance maintained, or required by this Contract to be maintained, by Supplier. Nothing in this section shall limit or affect Supplier's liability arising from claims brought by any third party.

    Notwithstanding the foregoing, in no event will Supplier's liability for a claim arising out of a security breach or data loss exceed the greater of three times the total amount payable to Supplier over the duration of the Contract prior to the event or circumstances that first gave rise to such liability, or $15,000,000.

33. **Obligations Beyond Contract Term.** The Statewide Contract shall remain in full force and effect to the end of the specified term or until terminated or canceled pursuant to the Statewide Contract. All obligations of the Supplier incurred or existing under the Statewide Contract as of the date of expiration, termination or cancellation will survive the termination, expiration or conclusion of the Statewide Contract.

34. **Counterparts.** The Agency and the Supplier agree that the Statewide Contract has been or may be executed in several counterparts, each of which shall be deemed an original and all such counterparts shall together constitute one and the same instrument.

35. **Further Assurances and Corrective Instruments.** The Agency and the Supplier agree that they will, from time to time, execute, acknowledge, and deliver, or cause to be executed, acknowledged, and delivered, such supplements hereto and such further instruments as may reasonably be required for carrying out the expressed intention of the Statewide Contract.

36. Transition Cooperation and Cooperation with other Suppliers. Supplier agrees that upon termination of this Statewide Contract for any reason, it shall provide sufficient efforts and cooperation to ensure an orderly and efficient transition of services to the State or another Supplier. The Supplier shall provide full disclosure to the State and the third-party Supplier about the equipment, software, or services required to perform services for the State. The Supplier shall transfer licenses or assign agreements for any software or third-party services used to provide the services to the State or to another Supplier.

Further, in the event that the State has entered into or enters into agreements with other Suppliers for additional work related to services rendered under the Statewide Contract, Supplier agrees to cooperate fully with such other Suppliers. Supplier shall not commit any act, which will interfere with the performance of work by any other Supplier.

37. State Security. Supplier shall obtain a criminal background investigation on its officers, agents, employees, subcontractor, or other workers ("Workers") assigned to have regular interaction with children, students, employees, money, sensitive or confidential data, or access to the State Entity's premises, computers, hardware, software, programs, and/or information technology infrastructure or operations. The State Entity reserves the right to require additional background checks to be made on any of Supplier's Workers. Supplier shall review the results of the background investigation. If such background investigation reveals or at any time Supplier discovers that a Worker has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, breach of trust/fiduciary responsibility, or which raises concerns about facility, system, or personal security or is otherwise job related, Supplier shall not permit that Worker to access any state facilities, data, or technology, shall remove any access privileges already given to that Worker, and shall not permit any such access unless Supplier notifies the State Entity and the state Entity expressly consents to the access, in writing, prior to the access. Supplier shall immediately notify the State Entity of any change in a Worker's criminal history. The State Entity may, in its sole discretion, terminate a Worker's access to the State Entity's facilities, computers, hardware, software, programs, and/or information technology infrastructure or operations. Supplier shall participate fully in the defense of, indemnify, and hold harmless the State Entity for its failure to obtain appropriate background investigations and for the actions of its Workers.

38. Sexual Harassment Prevention. The State of Georgia promotes respect and dignity and does not tolerate sexual harassment in the workplace. The State is committed to providing a workplace and environment free from sexual harassment for its employees and for all persons who interact with state government. All State of Georgia employees are expected and required to interact with all persons including other employees, Suppliers, and customers in a professional manner that contributes to a respectful work environment free from sexual harassment. Furthermore, the State of Georgia maintains an expectation that its Suppliers and their employees and subcontractor will interact with entities of the State of Georgia, their customers, and other Suppliers of the State in a professional manner that contributes to a respectful work environment free from sexual harassment.

Pursuant to the State of Georgia's Statewide Sexual Harassment Prevention Policy (the "Policy"), all Suppliers who are regularly on State premises or who regularly interact with State personnel must complete sexual harassment prevention training on an annual basis.

If the Supplier, including its employees and subcontractor, violates the Policy, including but not limited to engaging in sexual harassment and/or retaliation, the Supplier may be subject to appropriate corrective action. Such action may include, but is not limited to, notification to the

employer, removal from State premises, restricted access to State premises and/or personnel, termination of contract, and/or other corrective action(s) deemed necessary by the State.

(i) If Supplier is an individual who is regularly on State premises or who will regularly interact with State personnel, Supplier certifies that:

a. Supplier has received, reviewed, and agreed to comply with the State of Georgia's Statewide Sexual Harassment Prevention Policy located at http://doas.ga.gov/human-resources-administration/board-rules-policy-and-compliance/jointly-issued-statewide-policies/sexual-harassment-prevention-policy;

b. Supplier has completed sexual harassment prevention training in the last year and will continue to do so on an annual basis; or will complete the Georgia Department of Administrative Services' sexual harassment prevention training located at this direct link https://www.youtube.com/embed/NjVt0DDnc2s?rel=0 prior to accessing State premises and prior to interacting with State employees; and on an annual basis thereafter; and,

c. Upon request by the State, Supplier will provide documentation substantiating the completion of sexual harassment training.

(ii) If Supplier has employees and subcontractor that are regularly on State premises or who will regularly interact with State personnel, Supplier certifies that:

a. Supplier will ensure that such employees and subcontractor have received, reviewed, and agreed to comply with the State of Georgia's Statewide Sexual Harassment Prevention Policy located at http://doas.ga.gov/human-resources-administration/board-rules-policy-and-compliance/jointly-issued-statewide-policies/sexual-harassment-prevention-policy;

b. Supplier has provided sexual harassment prevention training in the last year to such employees and subcontractor and will continue to do so on an annual basis; or Supplier will ensure that such employees and subcontractor complete the Georgia Department of Administrative Services' sexual harassment prevention training located at this direct link https://www.youtube.com/embed/NjVt0DDnc2s?rel=0 prior to accessing State premises and prior to interacting with State employees; and on an annual basis thereafter; and

c. Upon request of the State, Supplier will provide documentation substantiating such employees and subcontractor' acknowledgment of the State of Georgia's Statewide Sexual Harassment Prevention Policy and annual completion of sexual harassment prevention training.

DATA SECURITY TERMS AND CONDITIONS

Attachment: 4

In the course of providing goods and/or services to the State of Georgia and governmental entities of the State pursuant to this contract, Supplier may gain access to Sensitive State Data as defined below. In such event, these Data Security Terms and Conditions shall apply.

I. DEFINITIONS AND GENERAL INFORMATION

A. Definitions. The following words shall be defined as set forth below:

1. **"Authorized Persons"** means Supplier and its employees, subcontractors, or other agents to the extent necessary for such persons to access Sensitive State Data to enable Supplier to provide goods and/or services under this Agreement.

2. **"Data Breach"** means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store, or dispose of data is breached and Sensitive State Data or information technology resources is exposed to unauthorized access, use, disclosure, alteration, or theft.

3. **"Personally Identifiable Information"** includes, but is not limited to, personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; Personal Information as defined in O.C.G.A. 10-1-911 and/or any successor laws of the State of Georgia; Personally Identifiable Information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; Medical Information as defined in Georgia Code Section 32.1-127.1:05; Protected Health Information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; Nonpublic Personal Information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.

4. **"Personal Data"** as defined in O.C.G.A. § 10-1-911 means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
   a. Social security number;
   b. Driver's license number or state identification card number;
   c. Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
   d. Account passwords or personal identification numbers or other access codes; or
   e. Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the

information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

5. **"Sensitive State Data"** means all Personally Identifiable Information and other information that is not intentionally made available by the State on public websites or publications, including but not limited to business, administrative, and financial data, intellectual property, and patient, student and personnel data and records not required to be publicly disclosed under the Georgia Open Records Act, O.C.G.A. § 50-18-72 et seq., including any plan, blueprint, or material which if made public would compromise security. Sensitive State Data includes data created or in any way originating with or on behalf of the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, Supplier's hardware or exists in any system owned, maintained or otherwise controlled by the State or Supplier.

6. **"Security Incident"** means the potentially unauthorized access by non-Authorized Persons to Sensitive State Data that could reasonably result in the use, disclosure, alteration, or theft of the Sensitive State Data or information technology resources within the possession or control of Supplier or any cyber-attack, data breach, or identified use of malware that may create a life-safety event, substantially impair the security of data or information systems, or affect critical systems, equipment, or service delivery. A Security Incident may or may not turn into a Data Breach.

II. DATA OWNERSHIP AND PROTECTION

A. Data Ownership. The State will own all right, title, and interest, including all intellectual property rights, in its data that is provided with respect to the goods and services provided under this Agreement. Supplier shall not access Sensitive State Data, except 1) as is reasonably necessary to perform data center operations, 2) in response to service or technical issues, 3) as required by Supplier to provide the goods and services covered by this Agreement or 4) at the State's request. Supplier has a limited, non-exclusive license to use Sensitive State Data solely for the purpose of performing its obligations under this Agreement.

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

1. Supplier shall maintain appropriate administrative, physical, and technical security measures to safeguard against unauthorized access, use, disclosure, alteration, or theft of Sensitive State Data. Such security measures shall be in accordance with current NIST 800-53 standards commensurate with the FISMA data classification specified by the State. If no data classification is specified by the State, in accordance with the measures applicable to the FISMA moderate classification.
2. Supplier shall use industry best practices and up-to-date security tools, technologies, and practices such as network firewalls, anti-virus protections, vulnerability scans, system logging, 24x7 system monitoring, third-party penetration testing, and intrusion detection methods in providing services under this Agreement.
3. Where the security objectives of confidentiality, authentication, non-repudiation, or data integrity are categorized FISMA compliance level moderate or higher, all electronic Sensitive State Data shall be encrypted using a cryptography method specified by the State while at rest on all devices controlled by Supplier and in transit across public networks with controlled access. Unless otherwise provided in the Agreement, Supplier is responsible for encryption of the Sensitive State Data.

4. Unless otherwise provided in the Agreement Supplier shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Sensitive State Data to that which is absolutely necessary to perform job duties.
5. Supplier shall not disclose Sensitive State Data to any third party without the prior written consent of the State except as otherwise provided by the Agreement or required by law. Nor shall supplier, copy, or retain Sensitive State Data except as provided for in the RFX. Supplier shall ensure that its employees and agents who will have potential access to Sensitive State Data have passed appropriate, industry standard background screening and, where applicable, federally mandated background screening and possess the qualifications and training to comply with the terms of this Agreement. Supplier shall promote and maintain an awareness of the importance of securing Sensitive State Data among Supplier's employees and agents.

C. Data Location. In providing goods and services to the State, supplier shall access, store, and process Sensitive State Data solely from location(s) or data centers in the U.S. and Supplier shall notify State of such locations. Storage of Sensitive State Data at rest shall be located solely in location(s) or data centers in the U.S. and Supplier shall notify State of such locations. Supplier shall not allow its personnel or Authorized Persons to store Sensitive State Data on portable devices, including personal computers, except for devices that are used and kept only at U.S. location(s) or data centers. Supplier shall only permit its personnel and consultants to remotely access Sensitive State Data as required to provide goods and services under this Agreement and shall only allow such remote access from locations within the U.S.

III. SECURITY INCIDENT AND DATA BREACH RESPONSIBILITIES
Supplier shall inform the State of any Security Incident or Data Breach.

A. Incident Response. Supplier may need to communicate with outside parties regarding a Security Incident or Data Breach, which may include contacting law enforcement, fielding media inquiries, and seeking external expertise as mutually agreed upon, defined by law, or contained in the Agreement. Discussing security incidents with the State should be handled on an urgent as-needed basis, as part of Supplier's communication and mitigation processes as mutually agreed upon, defined by law, or contained in the Agreement. Any contacting of law enforcement on matters regarding State systems or data must be followed by a report to the Georgia Information Sharing and Analysis Center (GISAC) at (404) 561-8497.

B. Security Incident and Data Breach Reporting Requirements. Upon becoming aware of a Security Incident or Data Breach, Supplier shall:

1. Promptly notify the State identified contact within twenty-four hours of discovery or sooner, unless shorter time is required by the Agreement or applicable law;
2. Fully investigate the Security Incident or Data Breach and cooperate fully with the State's investigation of and response thereto. Except as otherwise required by law, Supplier shall not provide notice of the Security Incident or Data Breach directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the State;
3. promptly implement necessary remedial measures reasonably determined by the State; and
4. document responsible actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
5. Supplier will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State's satisfaction.
6. Supplier shall quarantine the Data Breach, ensure secure access to Data, and repair IaaS and/or PaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result

in the State exercising its options for assessing damages or other remedies under this Contract.

IV. LIABILITY

A. If Supplier will under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Sensitive State Data known as Personally Identifiable Information, the following provisions apply: In addition to any other remedies available to the State under law or equity, Supplier shall reimburse the State in full for all costs incurred by the State in investigation and remediation of any Data Breach or Security Incident caused by Supplier, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; a website or toll-free number and call center for affected individuals required by law, providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Breach or Security Incident.

B. If Supplier will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Sensitive State Data known as Personally Identifiable Information, the following provisions apply: In addition to any other remedies available to the State under law or equity, Supplier will reimburse the State in full for all costs reasonably incurred by the State in investigation and remediation of any Data Breach or Security Incident caused by Supplier.

V. SECURITY

A. Data Center Audit. If applicable in the provision of the goods and services covered by this Agreement, Supplier shall ensure an independent audit or provide ISO 27001 certification of its data centers at least annually at its expense and provide a copy of the audit report upon request. A Service Organization Control (SOC) 2 audit report or approved equivalent (the ISO 27001 certification, State RAMP certification, or FedRAMP certification) sets the minimum level of a third-party audit.

B. Security Processes. Supplier shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and Supplier.

C. Encryption of Data at Rest. For data categorized as moderate or high in Federal Information Processing Standard 199, Supplier shall ensure confidentiality and integrity of information at rest consistent with security control SC-28, Protection of Information at Rest, using control enhancement 1, Cryptographic Protection, in NIST Special Publication 800-53.

VI. RESPONSE TO LEGAL ORDERS, DEMANDS, OR REQUESTS FOR DATA

A. Except as otherwise expressly prohibited by law, Supplier shall:

1. immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by Supplier seeking Sensitive State Data;
2. consult with the State regarding its response;
3. cooperate with the State's reasonable requests in connection with efforts by the State to intervene and quash or modify the legal order, demand, or request; and
4. upon the State's request, provide the State with a copy of its response.

B. If the State receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Georgia Open Records Act) or request seeking Sensitive State Data maintained by

Supplier, the State shall promptly provide a copy to Supplier. Supplier shall promptly supply the State with copies of data required for the State to respond and shall cooperate with the State's reasonable requests in connection with its response.

VII. TERMINATION OBLIGATIONS

A. Upon termination or expiration of the Agreement, Supplier shall implement In the State's sole discretion, a secure, orderly (1) destruction of, or (2) return of Sensitive State Data in the format and at a time specified by State. Transfer to State or a third party designated by State shall occur without significant interruption of service and, to the extent technologically feasible, State shall have access to Sensitive State Data during the transfer. Following such transfer, Supplier shall securely destroy Sensitive State Data in its possession or control. Supplier shall not destroy any Sensitive State Data that has not been returned to State in the event of ongoing contract or other disputes between the parties or for so long as amounts remain payable by State.

B. Destroyed Sensitive State Data shall be permanently deleted and shall not be recoverable in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization, using the purge method from Appendix A, Minimum Sanitization Recommendations, for the type of media being purged. Certificates of destruction shall be provided to the State. Supplier may retain a copy of Sensitive State Data if necessary to comply with law or its applicable professional standards.

VIII. COMPLIANCE

A. Supplier shall comply with all applicable laws and industry standards in providing goods and services under this agreement. Any Supplier personnel visiting the State's facilities will comply with all applicable State policies regarding access to, use of, and conduct within such facilities. The State shall provide copies of such policies to Supplier upon request.

B. Supplier warrants that in providing goods and services to the State it is fully compliant with relevant laws, regulations, and guidance that may be applicable to the goods and services such as: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.

C. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to the goods and services provided to the State, Supplier shall, upon written request, furnish proof of compliance with PCI-DSS within 10 business days of the Request.

IMPORTANT -- READ THIS AGREEMENT BEFORE USING OR ACCESSING ANY JUNIPER SOLUTIONS.

YOU SHALL HAVE NO RIGHT TO USE OR ACCESS ANY JUNIPER SOLUTIONS UNLESS YOU: (I) RECEIVED SUCH SOLUTIONS FROM AN APPROVED SOURCE; AND (II) CONSENT TO BE BOUND BY ALL TERMS OF THIS AGREEMENT, WHICH CONSENT IS EVIDENCED BY EXECUTING AN ORDER THAT REFERENCES THIS AGREEMENT.

IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF ANOTHER LEGAL ENTITY, YOU REPRESENT THAT YOU ARE AUTHORIZED TO BIND SUCH ENTITY TO THE TERMS OF THIS AGREEMENT, IN WHICH CASE "COMPANY" SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT AGREE WITH THESE TERMS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE OR ACCESS JUNIPER SOLUTIONS.

JUNIPER PURCHASE AND LICENSE AGREEMENT

*This Juniper Purchase and License Agreement (the "**Agreement**") is entered into between Juniper (as defined below) and the party accepting these terms ("**Company**") (each a "**Party**", collectively the "**Parties**"), and consists of the General Terms and Conditions, Schedule(s), Glossary, and other documentation incorporated into this Agreement.*

GENERAL TERMS AND CONDITIONS

1. **Scope.** *These General Terms and Conditions ("**GTC**") set forth terms and conditions for the purchase, use, access, or license of Juniper Solutions by Company during the Agreement Term (as defined below).*

2. **Precedence.** *In the event of any conflict, the order of precedence is* **for Juniper's documents is as follows,** *as applicable: (i) GTC and the Glossary; (ii) Schedule(s); (iii) Program Terms; (iv) Policies; and (v) Descriptive Content.*

Notwithstanding the above, the Parties may agree that a document prevails and takes precedence over any document ranked higher in the above order. In such case, such document shall explicitly reference the provision it modifies and will identify the revised order of precedence.

3. **Term.** *This Agreement is effective from the date of the last signature or when it is accepted by Company online (the "**Effective Date**") and will have an initial term of twelve (12) months immediately following the Effective Date ("**Initial Term**").*

4. **Transactional Terms.** *Where Company purchases or licenses Juniper Solutions directly from Juniper, Company will comply with the following terms:*

a) Payment. **Reserved, addressed in Statewide Contract.**

b) Ordering. **Reserved, addressed in Statewide Contract.**

c) Pricing. The purchase price for Juniper Solutions is **the discount** *set forth in Juniper's* **proposal applied to Juniper's** *then-current price list.*

d) Cancellations.

e) Delivery. Juniper shall deliver: (i) Hardware, in accordance with ***the Statewide contract*** *(ii) Software, when it is made available for download; (iii) Cloud Services, when it is made available for Use; (iv) Support Services, upon issuance of an activation notice; and (v) Professional Services, as specified in the applicable SOW.*

f) Taxes. **Reserved, addressed in Statewide Contract.**

5. **Company Affiliates.** If authorized by both Parties in writing, each Affiliate of Company is deemed to be a Party to this Agreement and Company guarantees the payment and performance of each Affiliate.

6. Confidentiality. **Reserved, addressed in Statewide Contract.**

7. **Intellectual Property. Reserved, addressed in Statewide Contract.**

8. **Intellectual Property Indemnity**. **Reserved, addressed in Statewide Contract.**

9. Limitation of Liability. **Reserved, addressed in Statewide Contract.**

10. Termination. Reserved, addressed in Statewide Contract.

a) Suspension. Juniper may suspend access to or use of Cloud Services, Software, or Services if: (i) it reasonably believes that Company's use is likely to cause harm to Juniper or a third party; (ii) Company defaults on payment obligations; or (iii) if the provision of Cloud Services, Software or Services as currently offered becomes prohibited by applicable Law.

b) Survival. Sections 4 (Transactional Terms), 10 (Termination), and 11 (Miscellaneous) survive termination of this Agreement.

11. Miscellaneous

a) Governing Law and Jurisdiction. **Reserved, addressed in Statewide Contract.**

b) Compliance with Laws and Policies. Each Party shall comply with all applicable Laws and Policies.

c) Export. Juniper Solutions are subject to U.S. and local export control and sanctions Laws. Company acknowledges and agrees to the applicability of and compliance with those Laws, and Company will not receive, use, transfer, export or re-export any Juniper Solutions in a way that would cause Juniper to violate those Laws. Company also agrees to obtain any required licenses or authorizations.

d) Force Majeure. **Reserved, addressed in Statewide Contract.**

e) Assignment. **Reserved, addressed in Statewide Contract.**

f) Notices. **Reserved, addressed in Statewide Contract.**

g) Audit. **Reserved, addressed in Statewide Contract.**

h) Severability; Remedies; Waiver. If any one or more provisions in this Agreement shall be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired. Except as otherwise expressly provided, the remedies are cumulative and in addition to any other remedies at law or equity. A Party's failure to enforce any provision of this Agreement shall not constitute a waiver of any future enforcement of that or any other provision of this Agreement.

i) No Third-Party Beneficiaries. Company acknowledges that the benefits of the rights granted to, and entitlements received by, it under this Agreement are strictly for itself, and for its Affiliates, as the case may be.

j) Entire Agreement; Amendment. All amendments to this Agreement must be in writing and signed by both Parties.

k) Translation. Where Juniper provides local language translations of this Agreement, those translations are provided for informational purposes only and the Parties agree that the English version of this Agreement will prevail.

CUSTOMER SCHEDULE

(Applies to all purchases of Joint Solutions for internal use)

1. Applicability. *This Customer Schedule contains additional terms and conditions applicable to the license, use, access, and purchase of Juniper Solutions by Company. In this Schedule, Section 2 applies to the purchase or license of all Juniper Solutions, and in the case of: (i) Hardware, Section 3 also applies; (ii) Services, Section 4 also applies; and (iii) Software or Cloud Services, Section 5 also applies.*

2. Terms for all Juniper Solutions

a) Transactional Terms. Company may not purchase Juniper Solutions directly from Juniper unless expressly authorized in writing by Juniper. Section 4 of the GTC applies only if Company is purchasing Juniper Solutions directly from Juniper and does not apply to Orders from an Authorized Reseller.

b) Onboarding Information. The Parties agree to provide Onboarding Information in support of this Agreement.

c) Use of Third-Party Products. Unless otherwise certified for use by Juniper, Company's use of Juniper Solutions with third-party products is at Company's own risk. Juniper shall not be responsible for support, warranties, or other terms applicable to such third-party products.

d) End of Life / End of Service. Juniper's End of Life and End of Service procedures will be actively communicated to Authorized users in accordance with the Statewide Contract.

e) Evaluation Terms.

f) Users. Company is responsible for all acts or omissions of its Users with respect to Juniper Solutions.

3. Specific Terms for Hardware

a) Hardware Warranty. **Reserved, addressed in Statewide Contract.**

b) Transfer. All transfers are subject to the inspection and reinstatement Policies available on Contract Resources.

4. Specific Terms for Services

a) Support Services (Maintenance Services, Advanced Services, Education Services).

i. Descriptive Content. Scope and details of Support Service-specific terms are specified in Descriptive Content.

ii. Subcontracting. Juniper may subcontract with, or assign to, its Affiliates or other third parties the obligations for performance of any Support Services.

iii. True Up. Company must promptly True Up any unpurchased Support Services rendered by Juniper.

b)Professional Services. Professional Services that are provided: (i) by Juniper to the Company directly will be set forth in a SOW governed by this Agreement; and (ii) to the Company through an Authorized Reseller, will be set forth in a SOW as agreed between Company and such Authorized Reseller.

c)Warranty. Juniper warrants that Services will be performed in a professional manner following industry standards.

5. Specific Terms for Software and Cloud Services

a) License and Right to Use. Subject to the terms and conditions of this Agreement (including the Licensing Guide), Juniper grants Company a non-exclusive, revocable, non-transferable (except under Section 5 of the GTC) license to Use the Software and right to Use the Cloud Services, during the applicable License Term, for up to the Licensed Units and solely for Company's internal business operations. Company has no right or license to Use the Software or Cloud Services unless Company rightfully purchased the right to Use the Software or Cloud Services from an Approved Source.

b) General Restrictions. Unless expressly authorized in writing, or except to the extent transfer may not be restricted under Law, Company shall not: (i) sublicense, transfer, or assign, any right or license to the Software or Cloud Services to any other person or legal entity; (ii) directly or indirectly decompile, disassemble, reverse engineer, modify, unbundle, or create derivative works based on any Software or Cloud Services; (iii) remove, modify, or conceal any product identification, copyright, or confidential notices or other marks; (iv) make any copies, except as reasonably necessary for archival purposes; and (v) Use or fail to restrict Use of the Software or Cloud Services in violation of applicable Law.

c) End of Entitlement. Upon cessation of the right to Use Software or Cloud Services, Company shall promptly cease using and accessing the Software or Cloud Services and delete, destroy, or return all copies of any Software and any Confidential Information to Juniper, and shall provide written certification that it has complied with this Section 5(c).

d) Third-Party Software. Software or Cloud Services may contain or otherwise make use of Third-Party Software that may be subject to separate license terms. Juniper warrants that Software or Cloud Services, when used in conformance with this Agreement, does not include Third-Party Software that restricts Company's usage rights granted under this Agreement.

e) Warranty. Juniper will provide Software and Cloud Services with commercially reasonable care in material conformance with the Statewide Contract, the **RFP, and the** *applicable Descriptive Content.*

f) Additional Software Terms. For Software:

(i) Juniper grants Company a license to Use Software Updates made available as part of the applicable Support Services for such Software or, if applicable, Hardware. The terms and conditions applicable to the Software also apply to any Update of that Software, and Company must track its Use of Software and True Up any unpurchased use.

(ii) In the limited event that licensed Software includes source code, (either as part of the Software or made available separately by Juniper, or is ancillary to the Use of Software), such source code is provided "as-is", without any warranty and for internal use only unless expressly licensed otherwise by Juniper.

a)Additional Cloud Services Terms. For Cloud Services:

(i) Company shall: (1) be solely responsible for the accuracy, quality, integrity and legality of Company Data; (2) prevent unauthorized Use of the Cloud Services, and notify Juniper promptly of any such unauthorized Use; (3) Use the Cloud Services in accordance with the Policies, Descriptive Content, and applicable Laws; (4) obtain any and all third-party consents necessary for the use and processing of Company Data in connection with the Cloud Services; and (5) Use the Cloud Services with only appropriately licensed and Juniper approved third party software and technology.

(ii) Company shall not: (1) Use the Cloud Services to store or transmit infringing, libelous, harmful or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights; (2) Use the Cloud Services to store or transmit Malicious Code; (3) interfere with or disrupt the integrity or performance of the Cloud Services or related third-party data ; and (4) permit any third party to access the Cloud Services.

6. Data Protection.

GLOSSARY

A. Definitions applicable to the General Terms and Conditions

"Advanced Services" means the services rendered by Juniper resident engineer or resident consultants.

"Affiliate" of a Party means, any entity and its successors controlled by, controlling, or under common control with, such Party, where "control" in any of the foregoing forms means ownership, either direct or indirect, of more than 50% of the equity interest entitled to vote for the election of directors or equivalent governing body. An entity remains an Affiliate as long as it continues to meet the foregoing definition.

"Authorized Reseller" means a reseller of Juniper Solutions that sells Juniper Solutions to Company pursuant to a valid contract with Juniper to conduct such resale activities.

"Cloud Services" means Juniper's generally available software-as-a-service offerings.

"Contract Resources" means the following website where Program Terms, Policies, and Descriptive Content are posted: https://uat-aem.juniper.net/us/en/legal-notices/juniper-networks-contracts-resource.html.

"CSD" or "Cloud Service Description" means a description of the Cloud Service, including the incorporated Support Services, Juniper's obligations in providing the Cloud Service, and any specific privacy and data protection information.

"Data Protection Addendum" or "DPA" means the then-current data protection addendum as set forth within the applicable Schedule.

"Descriptive Content" means the "Data Sheets," "Service Description Document(s)," or "Cloud Service Description(s)" made available on Contract Resources that describe the Juniper Solutions, as applicable.

"Education Services" means training and education services provided by Juniper.

"Hardware" means the physical components of Juniper's equipment delivered hereunder.

"Juniper" means, if Juniper Solutions are shipped, delivered or deployed by Juniper or an Authorized Reseller to a location in: (a) North America, Central America or South America, Juniper Networks (US), Inc.; (b) United Kingdom, Juniper Networks (U.K.) Limited; (c) India, Juniper Networks Solution India Private Limited; (d) Australia, Juniper Networks Australia Pty Ltd; or (e) where a location is not listed above, Juniper Networks International B.V., and for on-site Support Services, exclusively means the local Juniper contracting entity, which is the Juniper Affiliate that signs the SOW.

"Juniper Solutions" consists of, together or individually, Hardware, Software, Services and Cloud Services.

"Laws" means laws, ordinances, codes, rules, standards, and regulations of any territory or jurisdiction.

"Licensing Guide" means the guidelines published on Contract Resources pertaining to activation, installation, management, and monitoring of Software licenses.

"Maintenance Services" means the technical support services and maintenance provided by Juniper as more fully described in the applicable SDD or CSD.

"Onboarding Information" means information shared between Juniper and the Company (as updated from time to time) for the purposes of transacting under this Agreement.

"Policies" means, without limitation, any policies, guidelines, or procedures applicable to Juniper Solutions made available on Contract Resources that are effective as of the date of the Purchase Order.

"Processed Data" means Personal Data (as defined in the DPA) collected, processed, or used in connection with the provision of Juniper Solutions.

"Professional Services" means plan, build, migration, implementation, and optimization services set forth in a SOW.

"Program Terms" means any country, industry, channel, program, or product-specific terms and conditions made available on Contract Resources.

"Purchase Order" or "Order" means an order issued to and accepted by Juniper which is fully authorized by a Company representative and subject to the terms and conditions of this Agreement.

"Quote" means a quotation issued to Company or the Authorized Reseller for the purchase of Juniper Solutions.

"Schedule" refers to the terms and conditions applicable to Company's purchasing model and attached to the GTC.

"SDD" or "Services Description Document" means a document describing the associated Support Services.

"Services" means, collectively Maintenance Services, Advanced Services, Education Services, and Professional Services.

"Software" means the Juniper machine-readable object code and accompanying activation keys, if any, made available to Company, whether incorporated in the Hardware (e.g., firmware) or delivered separately, and includes Software Releases and any Updates of that Software the Company is entitled to through Maintenance Services.

"Software Release" means a new production version of the Software.

"Statement of Work" or "SOW" means a document executed by the Parties that references this Agreement and describes the scope and details of Professional Services that shall include at a minimum: (i) a reasonably detailed description of the project or services to be performed; (ii) a schedule and completion date; (iii) the description of who will perform the applicable services; (iv) an acceptance procedure for the services rendered; (v) a compensation and payment schedule; and (vi) the identity of the Company that will receive the benefit of the services.

"Tax" or "Taxes" means all taxes, levies, imposts, all custom and stamp duties, tariffs, import fees, fines or other charges imposed by any jurisdiction, country or any subdivision or authority arising out of this Agreement or any instrument or agreement otherwise required, and all related interest, penalties or similar liabilities, except such taxes as are imposed on or measured by a Party's net or gross income, capital, net worth, franchise, privilege, or property.

"Third-Party Software" means any software (including object code, binary code, source code, interpreted code, script code, firmware, drivers, microcode, application programming interfaces, web services, software development kits, subroutines or other code, and including commercial, open-source and freeware software) and any documentation or other material related to such software, and any derivative of any of the foregoing, that is not majority owned by Juniper.

"Update" means updates, fixes, corrections, enhancements and other modifications to the Software or Cloud Service.

B. Definitions applicable to the Customer Schedule

"Approved Source" means Juniper or an Authorized Reseller.

"Company Data" means all information submitted by Company to Juniper and may include third-party data.

"License Metric" means a unit of measurement that restricts the use of the Software or Cloud Service (e.g., Network Element or Node, or any other metric set forth in a SKU or other notification).

"License Term" means the period during which the Company is permitted to Use the Software or Cloud Services.

"Licensed Units" mean a number of units under a License Metric that limits the Use of the licensed Software or Cloud Services (e.g., 10M, 50 Nodes, or any other units under a License Metric set forth in a SKU or other notice).

"Malicious Code" means viruses, worms, time bombs, trojan horses and other harmful or malicious code, files, scripts, agents, programs, or any identifying information or other metadata associated with them, such as suspected malicious website, URL, or IP addresses.

"Network Element" or "Node" means a physical or virtual device recognizable by the Software as a unique device that the Software may directly or indirectly administer, monitor, manage, provision, or configure.

"Perpetual License" means a license with a perpetual License Term.

"SKU" means a stock-keeping unit or unique identifier for each distinct product and service that can be purchased and any summary description of such product or service.

"Subscription" means a license to Use the Software or the Cloud Services solely during a fixed License Term.

"Support Services" means, collectively Maintenance Services, Advanced Services, and Education Services.

"True Up" means a reconciliation by Company of its deployment or Use of unpurchased or unlicensed Juniper Solutions.

"Use" and "Used" means: (a) for Software, to install, use, access, activate, or view the Software in executable form; and (b) for Cloud Service, to access that Cloud Service.

"Users" means employees, consultants, contractors, and agents authorized to Use the Software or Cloud Services under valid Subscriptions or Perpetual licenses.

Performance Requirements Document (PRD)

Introduction

The State of Georgia has identified the minimum standards and requirements to successfully meet the Networking needs of Georgia government. The purpose of this document is to facilitate understanding of these expectations and to provide a basis for a collaborative relationship and for managing continuous improvement opportunities.

Solicitation Intent

The purpose and intent of this eRFP are to establish a statewide source of supply and services for Networking Equipment and Related Services and to identify qualified Suppliers that have the depth, breadth, and quality of resources necessary to meet all the standards of the State, to deliver a wide variety of Networking Equipment and Related Services to a broad and dispersed demographic of state and local government users, who require a high level of customer care before and after the sale.

DOAS desires to award contracts to responsive and responsible Suppliers (Original Equipment Manufacturers (OEM)), whose bid proposals provide the best value and services to state and local agencies. DOAS expects to award multiple contracts in each category that are (1) within a competitive range and/or (2) provide adequate sources of supply throughout the State of Georgia.

The State expects that the awarded Supplier(s) in each Networking Equipment Category shall furnish high-quality, innovative Networking equipment and related services at the lowest price available while maintaining or exceeding current service and performance level(s). The State expects Suppliers' products and Suppliers' sales, customer service teams, Authorized Servicing Partners, contract management process, and quality management systems to be "best-in-class".

Suppliers should be able to provide a broad range of hardware/software products as well as related service offerings to all Authorized Users of the State of Georgia. Suppliers may sell their products and services directly via their own sales force and indirectly through a network of Authorized Servicing Partners.

Relevant History

The current contract, IT Networking Equipment (99999-SPD-T20120501), a convenience contract, was awarded and effective June 1, 2012, with nine (9) awarded Suppliers across five (5) categories.

Category 1 - Wired Networking & Infrastructure Products
Category 2 - Network Optimization & Management Products
Category 3 - Wireless Networking & Infrastructure Products
Category 4 - Security Products
Category 5 - Unified Communications Products

Via this sustainable, flexible, and well-established contract, the State of Georgia has seen cost savings through significantly lower product costs, improved product performance and reliability, improved relationships with contract Suppliers and their Servicing Partners, and increased access to value-added technology/best-in-class products.

The new contract aims to ensure and continue all the above-mentioned successful contract implementations while focusing on improving and expanding the contract in the following, including but not limited to:

- Category scope
- Software and Management Solutions
- Security
- Related Value-Added Services
- Internet of Things (IoT) products
- Increased cost transparency

In addition to the IT Networking Equipment contract, in 2019, the State negotiated and awarded a participating addendum (PA), via the NASPO ValuePoint Consortia for Data Communication Products and Services (99999-SPD-NVPUT3229-0001). The resulting statewide contract will serve as a consolidation of the two existing contracts.

The State has done extensive research into the category of Unified Communications and has concluded that this category has developed and expanded in the past couple of years to where it is now a separate market with separate requirements and a separate set of Suppliers providing these services. Suppliers in this market can provide the foundation for advanced unified communications providing services such as Unified Communications as a Service (UCaaS), cloud services, session management, collaborative contact centers, voice, video, messaging, mobility, and meeting solutions (i.e., web, audio, IM&P, file sharing, white boarding, guest support, etc.). Therefore, the State has made the decision to exclude this category in the new Networking Equipment and Related Services contract and instead focus and continue the research to establish a separate Unified Communications contract in the future.

Through spend analysis encompassing fiscal years 2020-2023 (July 1, 2019 – June 30, 2023), Authorized Users of the current statewide contract spend, on average, approximately $42.3M annually on the equipment and services outlined in this eRFP. Please see section 1.3 of **Attachment A. Statewide Contract eRFP Instructions & Guidelines** for further spend data details.

Category Details

The equipment and services pursuant to this eRFP have been separated into three (3) separate product/equipment categories, detailed below in Table 1:

Table 1

Network Product/Equipment Categories

Category # & Name	Category 1 Core Networking & Infrastructure Products	Category 2 Network Optimization & Management Products	Category 3 Network Security Products & Security Solutions
Category Equipment Details **Mandatory Products**	This category includes all equipment, components, and management solutions necessary for wired and wireless (Cellular and Wi-Fi) networking infrastructures and solutions, inclusive of, but not limited to: • Ethernet-based switches • Core / Edge Router • Wireless Access Points (Indoor and Outdoor)	This category includes all equipment, components, and management solutions necessary to monitor, manage, and improve network performance, inclusive of, but not limited to: • Network Observability / Management Solutions	This category includes all equipment, components, and management solutions related to network security equipment and network security solutions, inclusive of, but not limited to: • Network Firewall
Category Equipment Details **Additional In-Scope Products**	• All types of Switches, Routers, Hubs, and Modems • Wired and wireless network infrastructure products that support Wired Local Area Network (LAN) • Wired and wireless network infrastructure products that support Wide Area Network (WAN) • Campus Networks hardware/appliances • Gateways • Interface modules • Associated network management software • Dense Wavelength Division Multiplexing (DWDM) • Policy management tools • Non-Climate Controlled Solutions • Wireless Network Extenders and Repeaters • Wireless IoT devices, such as Temperature Sensors • Wireless bridges • Non-network specific Wireless radios (both internal and external, as well as other frequency radios used for digital networking) • Wireless Campus hardware/appliances • Wireless gateways • Cellular Repeaters • Cellular equipment related to LTE and 5G. • Small Cell Products • Wireless Controller/Management Products	• Specialized bandwidth management/WAN Optimization • Network device configuration management products/appliances • Network/application monitoring/diagnostics products/appliances • Load balancing equipment. • Dynamic Host Configuration Protocol (DHCP) • Domain Name System (DNS) • Network Traffic Analyzers • Virtual Networking Optimization Products and Solutions • Automation and Orchestration Protocol • IP Address Management Product	• Advance Web Access Firewall • Intrusion Prevention Systems • Unified Threat Management • Advanced Network Threat Prevention • Network Access Control • Cloud Access Security Brokers • DDoS Mitigation • Network Behavior Detection • SD-WAN • SASE • Endpoint Security • Content Filtering • Micro-Segmentation Solutions • Zero-Trust Network Access • Penetration Testing Tools • Data Loss Prevention • Other security appliances – both stand-alone and integrated. • Virtual Private Network (VPN) Products

Software and Management Solutions	Each specific category includes all software (on-prem, cloud, or hybrid), network management software, and network management and automation solutions required for core product function or full functionality of equipment and solutions in the category scope. **Please see Section 1) f) Software, Cloud Networking, Management and Automation Solutions of this document for details and requirements.** NO STANDALONE SOFTWARE OR MANAGEMENT SOLUTIONS SHOULD BE SOLD. (Software purchased as an independent solution not tied to a network product or network solution, should not be sold)
Related Value-Added Professional Services	All categories include all necessary related services, including but not limited to consulting/design, installation, configuration, maintenance/extended warranty, training, and relocation of networking equipment. **Please see Section 1) h) Related Valued-Added Services of this document for details and requirements.**
IoT Products	Each category allows for Internet of Things (IoT) products. These products must be an IoT product that can be deployed within, upon, or integrated into a State agency's physical asset to address government line of business needs. Proposals are expected to include IoT products designed to support common government lines of business in specific subcategories i.e., routers, switches, endpoints, network intrusion, detection, and performance sensors etc. IoT products can only be provided in categories that the Supplier is awarded in and can include endpoints that support items in that category.
Cloud Networking	Where applicable within each category, as it pertains to Network as a Service (NaaS), Infrastructure as a Service (IaaS), together with hybrid and multi-cloud network architecture solutions are within the scope of this RFP. Platform as a Service (PaaS), or Software as a Service (SaaS) products are only within scope when required for core product function or full functionality of equipment and solutions in the category scope. **Please see Section 1) f) iii) Cloud Networking Solutions of this document for details and requirements.**

1) Network Product/Equipment, Software, and Related Value-Added Professional Service Offerings (Applicable to all Categories)

a) Products / Equipment / Solutions

i) Please refer to Table 1 of this document for Category details and in-scope products. For the Category or Categories Supplier is responding to, Supplier must provide the mandatory stated listed products, and all additional in-scope products are preferred.

ii) Third-Party (3rd Party) Products and Solutions
   (1) Supplier agrees to provide a list, including functionality and other details, for all 3rd party compatible and interoperable products that Supplier can provide within the scope of the category or categories. Supplier should address:
      (a) Protocol details of how those 3rd party products will be supported by Supplier once installed in an Agency's networking infrastructure solution.
      (b) Products interoperability and compatibility with other products and how these products can assist in Authorized User's infrastructure.

iii) Open Networking Products
   (1) It's the desire and of high importance for the State to have the ability to purchase networking hardware without the requirement of Supplier-specific software or Supplier Partner-specific software for the hardware to function.
   (2) Supplier agrees to provide a list, including functionality and other details, for all Open Networking compatible and interoperable products that Supplier can provide within the scope of the category or categories. Supplier should address:
      (a) Protocol details of how those Open Networking products will be supported by Supplier once installed in an Agency's networking infrastructure solution.
      (b) Products interoperability and compatibility with other OEMs and how these products can assist in Authorized User's infrastructure, specifically focusing on lower cost, flexibility, scalability, reusability, and automation.
      (c) Details of how Supplier will work with other OEMs to collaborate and support these products.
      (d) Describe how Open Networking products fit into your research and development plan, including, creation of new partnerships, foster interoperability, and providing cost-effective solutions for your customers.

iv) IoT Devices
   (1) These products must be an IoT product that can be deployed within, upon, or integrated into a State agency's physical asset to address government line of business needs. Proposals are expected to include IoT products designed to support common government lines of business in specific subcategories i.e., routers, switches, end points, network intrusion, detection, and performance sensors etc. and can include endpoints that support items in this category.

b) Peripherals

i) Each category includes network peripherals and accessories necessary to the functionality of the network and/or to fully implement the solution such as transceivers, fiber cable, network interface cards, powers supplies, etc.

c) Catalog Offerings

i) After award, Supplier(s) will have the capability of offering their entire catalog of product that falls within the category scope.

ii) Supplier should provide entire product and service catalog offering, including extended warranties, service agreements, managed services etc., available to Authorized Users applicable to awarded category or categories.

d) Emerging technology

i) The State acknowledges that network technology, related services, and software solutions will evolve throughout the contract term of this contract, if those emerging technologies and solutions fit within the category scope of this RFP, Supplier, and its Authorized Servicing Partners are authorized to sell those items.

e) Hardware / Product / Equipment Licensing

i) Each category includes all necessary licenses and licensing models necessary to fully operate the category-specific equipment, products, and solutions.

ii) Supplier agrees to provide a detailed list of all licensing offerings including but not limited to:
(1) Specific licensing details, and how the license ties into the functionality of the product.
(2) Term length options
(3) Any cloud management license options
(4) License transferability options
(5) Any co-term license options
(6) Manageability and visibility options
(7) Subsequent year pricing details
(8) Bandwidth increases capabilities throughout the license term.
(9) Life cycle management
(10) Pricing models and pricing options
(11) Multi-year subscription options

f) Software, Cloud Networking, Management and Automation Solutions

i) Software Products and Solutions
(1) Supplier shall provide software (on-prem, cloud, and/or hybrid), required for core product function or full functionality of equipment and solutions in the category scope.
(2) Supplier is required to provide post-sale support on annually renewable software products.
(3) communicate changes in licensing structure, type, and service programs as early as possible.
(4) Product maintenance, updates, upgrades, and enhancements must be coordinated and managed with the Authorized Users to avoid work stoppage and keep users current on product upgrades and changes.

ii) Network Management Solutions
(1) Scope Includes all network management solutions (on-prem, cloud, or hybrid), required for core product function or full functionality of equipment and solutions.

iii) Cloud Networking Solutions
(1) Where applicable within each category, as it pertains to Network as a Service (NaaS), Infrastructure as a Service (IaaS), together with hybrid and multi-cloud network architecture solutions are within the scope of this RFP.
Platform as a Service (PaaS), or Software as a Service (SaaS) products are only within scope when required for core product function or full functionality of equipment and solutions in the category scope.
(2) The Supplier shall give advance notice (as agreed to by the parties and included in the SOW and/or SLA) to Authorized User the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that is expected to materially or negatively impact

service availability and performance, as well as any planned downtime for such upgrades.

(3) Supplier agrees that all cloud service, cloud solutions, and/or cloud infrastructure projects and integrations should be detailed and outlined using a comprehensive Scope/Statement of Work document (SOW) and should be accompanied by a cloud service level agreement (SLA). The SOW should clearly state all necessary steps and requirements of the project and the process to fully achieve the Authorized User's project goals. Please see section 3) g) of this document for additional project and SOW requirements.
   (a) The cloud SLA should establish a mutual understanding of the services, relationship between Authorized User and Supplier, prioritized areas, responsibilities, guarantees, and warranties provided by the Supplier. It should clearly outline metrics and responsibilities among the parties involved in cloud configurations, such as the specific amount of response time to report or address system failures.
   (b) The cloud SLA should include details regarding:
      (i) responsibilities of each party,
      (ii) the acceptable performance parameters,
      (iii) a description of the applications and services covered under the agreement,
      (iv) procedures for monitoring service levels, including speed, responsiveness, and efficiency,
      (v) a schedule for the remediation of outages,
      (vi) provisions for scalability of Cloud Services and any variation in fees or costs as a result of any such scaling,
      (vii) volume and quality of work (including precision and accuracy).

(4) The technical and professional activities required for managing and maintaining the Cloud Services are the responsibilities of the Supplier. The system shall be available 24/7/365 (with agreed-upon maintenance downtime) and shall provide service to customers as defined in the SOW.

(5) Public Cloud Connectivity Options
   (a) If Supplier can provide connectivity to hosted public cloud providers, Supplier should provide details of those options:
      (i) Microsoft Azure ExpressRoute
      (ii) AWS Direct Connect
      (iii) Google Cloud Interconnect
   (b) In addition to agreeing to and following all data and cloud security requirements already stated, Supplier agrees to provide cloud encryption security processes for all cloud connectivity services.

iv) Business Continuity, Disaster Recovery, and Geographic Redundancy Details

(1) Supplier agrees to provide a state/regional cloud network map for outage and redundancy purposes.

v) Cloud Networking Security Requirements

(1) Suppliers should provide Authorized Users with similar levels of security in the cloud as provided for on-prem infrastructures. Supplier's cloud networking security must have the following key capabilities:
   (a) Full Network Security Stack
   (b) Zero Day Protection
   (c) SSL/TLS Traffic Inspection
   (d) Network Segmentation
   (e) Unified Security Management
   (f) Automation

(g) Secure Remote Access
(h) Content Sanitization
(i) Third-Party Integrations
(j) Identity and Access Management Controls

vi) Network Automation Solutions
(1) Scope includes all network automation solutions (on-prem, cloud, or hybrid), required for core product function or full functionality of equipment and solutions.

g) Service and Maintenance

i) Suppliers should have service and maintenance offerings, standard and customizable to Authorized Users' needs specific to the category scope.
ii) Subject to Supplier's approval and the certifications held by its Authorized Servicing Partners, many Authorized Servicing Partners can also offer and provide Service and Maintenance Services at competitive pricing, along with local presence and support. As the awarded Supplier, Supplier is ultimately responsible for the service and performance of its Authorized Servicing Partner.

h) Related Value-Added Professional Services

Supplier shall, either direct, via Authorized Servicing Partners, or both, provide the following related value-added professional services for procurement at the time of product purchase or anytime afterward.

All professional services, including but not limited to, Installation, maintenance, and repair services must be performed by OEM-certified engineers or technicians, as well as ANSI/TIA-568 and IEEE 802 certified engineers or technicians if applicable.

This provided list of value-added services is not intended to be exhaustive:

(1) Maintenance Services
(a) Technical support, software maintenance, flexible hardware coverage, and smart, proactive device diagnostics for hardware.
(2) Engineering Services
(a) Technology professional who is highly skilled in maintaining the connectivity of networks in terms of data, voice, calls, videos, and wireless network services.
(3) Installation Services
(a) Basic installation and configuration or end-to-end integration and deployment.
(4) Deployment Services
(a) Survey/Design
(i) Discovery, design, architecture review/validation, and readiness assessment.
(b) Optimization
(i) Assessing operational environment readiness, identifying ways to increase efficiencies throughout the network, and optimizing Authorized Users infrastructure, applications, and service management.
(5) Remote Management Services
(a) Continuous monitoring, incident management, problem management, change management, and utilization and performance reporting that may be offered on a subscription basis.
(6) Consulting/Advisory Services
(a) Assessing the availability, reliability, security, and performance of Authorized Users' existing solutions.
(7) Networking Architectural Design Services

(a) Developing architectural strategies and roadmaps for transforming Authorized User's existing network architecture and operations management.

(8) Solution Implementation Services
   (a) Authorized User-specific tasks to be accomplished and/or services to be delivered based on Authorized User's business and technical requirements.

(9) Testing Services
   (a) Testing the availability, reliability, security, and performance of Authorized User's existing solutions

(10) Training Services and Knowledge Transfer
   (a) Supplier shall deliver modernized world-class learning programs and offer technical training that provides networking professionals with methods to properly configure, deploy, manage, and troubleshoot their network environments including Self-paced videos, Instructor-led training (ILT), and Onsite instructor-led classes. Supplier agrees to provide learning offerings for Authorized Users employees on networking technologies, including but not limited to designing, implementing, operating, configuring, and troubleshooting network systems pertaining to items provided under the contract.

(11) Additional Authorized Servicing Partner Services
   (a) Subject to Supplier's approval and the certifications held by its Authorized Servicing Partners, many Authorized Servicing Partners can also offer some or all the Services as listed above at competitive pricing, along with local presence and support. As the awarded Supplier, Supplier is ultimately responsible for the service and performance of its Authorized Servicing Partner.

2) Category-Specific Requirements

a) Category 1 – Core Networking & Infrastructure Products

The core network provides connectivity and routing services, wired or wireless, between different parts of the network and controls the flow of traffic between these parts.
In a wired network, data flows over cables. The cables connect to an interface card in an end device at one end and to an Ethernet port on the network switch or router at the other end.
In a wireless network, data flows over the air via radio waves. These signals travel from the end device to a wireless access point, which is connected to the network. This allows users to roam, untethered to wires or cables. That said, the wireless network still needs wired hardware components, like Ethernet switches, to support the wireless access points.

i) **Products / Equipment / Solutions**
   (1) **Please refer to section 1) Network Product, Software, and Related Value-Added Professional Service Offerings and Table 1 of this document for listed Category 1 in-scope products and details. Suppliers must provide the mandatory stated listed products, and all additional in-scope products are preferred.**

ii) **Category 1 Requirements**
   (1) Any products not offered by any statewide contract supplier under the resultant statewide agreements are considered out of scope.
   (2) Supplier agrees to remain compliant with and maintain all General mandatory requirements and all requirements applicable to category 1, listed in this document throughout the term of the contract.
   (3) Supplier agrees to remain compliant will all wiring standards and protocols, including, ANSI/TIA-568.
   (4) Supplier agrees to remain compliant with all IEEE 802 ethernet standards related to wired and wireless networking equipment.

(5) Supplier agrees to remain compliant with all IEC Ingress Protection (IP) ratings related to wired and wireless networking equipment.
(6) Power over Ethernet (PoE)
(a) Supplier agrees to remain compliant with all IEEE 802.3 PoE standards related to wired and wireless networking equipment.

b) Category 2 – Network Optimization & Management Products

Network optimization is an umbrella term that refers to a range of tools, strategies, and best practices for monitoring, managing, and improving network performance.

i) **Products / Equipment / Solutions**
(1) **Please refer to section 1) Network Product, Software, and Related Value-Added Professional Service Offerings and Table 1 of this document for listed Category 2 in-scope products and details. Suppliers must provide the mandatory stated listed products, and all additional in-scope products are preferred.**

ii) **Category 2 Requirements**
(1) Any products not offered by any statewide contract supplier under the resultant statewide agreements are considered out of scope.
(2) Supplier agrees to remain compliant with and maintain all General mandatory requirements and all requirements applicable to category 2, listed in this document throughout the term of the contract.

c) Category 3 – Network Security Products and Security Solutions

Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. Network security is important because it keeps sensitive data safe from cyber-attacks and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber-attacks, like distributed denial of service.

i) **Products / Equipment / Solutions**
(1) **Please refer to section 1) Network Product, Software, and Related Value-Added Professional Service Offerings and Table 1 of this document for listed Category 3 in-scope products and details. Suppliers must provide the mandatory stated listed products, and all additional in-scope products are preferred.**

ii) **Category 3 Requirements**
(1) Any products not offered by any statewide contract supplier under the resultant statewide agreements are considered out of scope.
(2) Supplier agrees to remain compliant with and maintain all General mandatory requirements and all requirements applicable to category 3, listed in this document throughout the term of the contract.

3) General Mandatory Requirements – Applicable to all Suppliers submitting a response to this eRFP.

a) Authorized Servicing Partner Management

The State intends that Suppliers seek their best Authorized Servicing Partners regarding their additional discount off the Suppliers' price, expert technical advice, proficient installation technicians, and excellent repair and warranty performance. The State also desires to procure

products and services in such a way that local, small, minority-, women-, and/or veteran-owned enterprises can effectively compete for the State's business.

Therefore, Suppliers utilizing Partners are expected to recommend the use of one or more Authorized Servicing Partners that meet or exceed the performance requirements of this eRFP. Suppliers are required to work with the State/DOAS to finalize the list of Authorized Servicing Partners that will be available to offer their services under the statewide contract (SWC). On behalf of their Authorized Servicing Partners, the State expects the Manufacturers to manage the following requirements at their partner level:

i) Supplier shall remain responsible for Authorized Service Partners' performance under the awarded Statewide contract.
ii) Post-award and on an on-going basis, Suppliers need to work with the State of Georgia to:
   (1) properly onboard Authorized Servicing Partners such that they are fully aware of statewide contract parameters,
   (2) maintain an Authorized Servicing Partner list and communicate with the State of Georgia any changes to the list,
   (3) obtain any applicable compliance documents,
   (4) validation of Authorized Servicing Partner's insurance coverage,
   (5) have an ongoing management and issue resolution process,
   (6) monitor service performance and customer satisfaction to ensure the Authorized Servicing Partners meet all the requirements listed in the RFP,
   (7) manage de-certification or off-boarding of partners from servicing statewide entities under this contract,
   (8) resolve customer escalated issues and,
   (9) in accordance with section 3.1 of Attachment A. Statewide Contract eRFP Instructions Document, provide the Contract Manager with a Subcontractor Report annually.

b) Ordering, Shipping, and Delivery

The global supply chain issues have affected all industries and markets. Three of the most critical challenges facing global supply chains are: labor shortages, equipment availability, and the ripple effect of global bottlenecks. The State desires Suppliers that can navigate, manage, and adjust to these issues while still servicing the State and its Authorized Users.

i) Supplier or its Authorized Servicing Partners shall, upon receipt of Purchase Order, provide Authorized User with an estimated time of delivery and shall keep Authorized User up to date on any changes to the timeline.
ii) Supplier or its Authorized Servicing Partners shall list the applicable purchase order number on all invoices and packing slips.
iii) Suppliers or Authorized Servicing Partners quotes should list awarded Supplier's assigned Statewide Contract number and must include a detailed breakdown of cost for equipment and/or services (model numbers, specific versions of equipment, misc. materials, etc.) Supplier shall not itemize quotes as generalized line items that group more than one cost element together. Supplier shall not hide any details contributing to the end price to the Authorized User.
iv) Supplier agrees that all Networking projects and integrations should be detailed and outlined using a comprehensive Scope/Statement of Work document (SOW). Please see section 3) g) of this document for additional project and SOW requirements. Each phase/milestone of the project should also clearly indicate the line-item price of each component included in each phase. Milestone payments are allowed for Networking Projects but should be fully agreed upon by both Authorized User and Supplier before the project can commence. Authorized User and Supplier shall both sign off on the acceptance of the project for each milestone phase before any payment is made.

v) Supplier agrees to maintain a data policy compliant, virtual, product catalog containing descriptions and pricing to easily identify what products are available and applicable contract discounts. The virtual catalog is intended to be an easily updated price file that will replace the excel spreadsheets suppliers provide under the current contract. It will not need to integrate with a purchasing system to execute orders. Only to provide Authorized Users way to easily identify what products supplier is offering, the cost of those products and the applicable discount.
   (1) continuously refresh product catalog to ensure variety and long-term viability.
   (2) update catalog as products are added/removed by supplier.
   (3) include a brief description of product uses and functions.
   (4) provide super user access for DOAS Contract Manager allowing them to view the virtual catalog and validate items are in scope as well as quotes and orders for all Authorized Users
   (5) include educational discounts, where applicable.
   (6) exclude products that aren't compliant with contract terms.

vi) All product deliveries will be F.O.B. destination and shipping charges must be included in the proposed discount price.

vii) Any Supplier and/or Authorized Servicing Partners term/condition added/inserted in a quotation or purchase order that tries to override the Statewide contract terms and conditions are unenforceable.

viii) All pricing or billing related to travel and/or lodging must be itemized in a quote at the point of sale. In addition, if the Supplier is billing for travel and/or related expenses it must be aligned with the state's current travel policy or as it may be amended from time to time. Suppliers can review the State's travel policy at https://sao.georgia.gov/travel/state-travel-policy.

c) E-Rate Compliance

i) If Supplier and/or Suppliers Authorized Servicing Partners have chosen to participate in the E-Rate program, the following applies:
   (1) E-Rate Participating Supplier and/or its Authorized Servicing Partners agree to remain compliant with all provisions of the Federal Communications Commission E-Rate program (Universal Service Program for Schools and Libraries) discount program established under the authority of the Federal Telecommunications Commission Act of 1996.
   (2) To the extent the equipment and services offered under this contract are subject to and eligible for the E-rate discount program, participating Suppliers must provide the equipment and services without the addition of any service or administration fee by the Supplier.

d) Customer Service

The State desires Suppliers together with their Authorized Servicing Partners to provide a high level of customer service support, before and after the sale of goods/services as well as effective administrative and internal operations to efficiently service Authorized Users of the State. These inquiries include product information, billing questions, disputes, delivery disputes, product returns, pricing information, adding, or deleting account names, addresses, phone numbers, and training requests.

Customer service in this case is also defined as Tier 1 support, where personnel are expected to answer general and product-related questions and provide basic assistance for most of the Authorized Users' concerns. If needed, Tier 1 support personnel agents should

be able to transfer and escalate to specific departments or teams, such as Tech Support and Incident Response Teams. At a minimum, the support should include:

i) Customer Service Requirements
   (1) Supplier agrees to provide a local account manager, preferably a Technical Account Manager (TAM).
      (a) The account manager shall have specialized knowledge of the Supplier's corporate operations, contract management systems, data security and practices, privacy responsibilities, helpdesk capabilities, maintenance operations, billing, and all other requirements necessary to fulfill Supplier's responsibilities.
   (2) Supplier agrees to provide the phone number to the local technical account manager as well as a general customer service/technical support number.
   (3) Supplier agrees to provide a complaint escalation procedure.
   (4) Supplier shall provide the following types of Customer Service options:
      (a) Manned telephone support by English-Speaking personnel
      (b) Monitored Email Support
      (c) Remote assistance using Remote Desktop and a Virtual Private Network where available.
   (5) Location of customer support centers and customer service personnel.
      (a) Customer Service Support – Onshore and/or Offshore

   (6) Telephone Support
      (a) 8:00 A.M. to 5:00 P.M. EST Monday – Friday
      (b) The service provider will respond to and acknowledge customer service-related inquiries, incidents, and requests submitted by the Authorized User within 24 hours after initial contact unless immediate after-hours support or technical support service need or incident response priority level accompanies the request. **See further below for priority-level descriptions and applicable response times.**

   (7) Email Support
      (a) Monitored 8:00 A.M. to 5:00 P.M. EST Monday – Friday
      (b) The Service Provider will respond to and acknowledge, customer service-related inquiries, incidents, and requests submitted by the Authorized User within 24 hours after initial contact unless immediate after-hours support or technical support service need or incident response priority level accompanies the request. **See further details below for priority-level descriptions and applicable response times.**

e) Technical Support Services and Incident Response Requirements

In addition to regular customer service support, Supplier shall, either direct, via Authorized Servicing Partners, or both, provide Technical Support and Incident Response Support.

Technical support

Supplier must have a robust multi-level tech support system where technicians, engineers, and other tech support personnel can provide solution driven support to Authorized Users in the most efficient way possible. Supplier shall clearly state how Authorized Users can escalate a tech support ticket to the next level or highest possible level when Authorized Users feel the need arises to escalate the ticket. At a minimum, the support should include:

i) **Technical Support Services**
   (1) 24/7/365 Tech Support Services (24 hours per day, 7 days per week, 365 days out of the year tech support. Constant, without interruption, including holidays.)

(2) Ticketing System
  (a) The ticketing system should include and offer the following:
    (i) Ticket prioritization based on criticality.
    (ii) Insight and view into the status of submitted tickets and the history of previously submitted tickets.
    (iii) Push notification's ability either via email, text, and/or mobile application.
      1. Status updates should include a documented workflow of the ongoing ticket details, potential scheduled meeting times with the engineer or service technician, if applicable, etc.
    (iv) Tickets should not be closed until fully resolved.

(3) Maintenance Support
  (a) Technical support, software maintenance, flexible hardware coverage, and smart, proactive device diagnostics for hardware.
  (b) Supplier should have and provide details of their process for scheduling onsite maintenance.

(4) Technical Support Location
  (a) Tier 1 – Onshore
  (b) Tier 2 – Onshore
  (c) Tier 3 – Onshore
  (d) Any additional tiers – Onshore

(5) Priority Levels for Tech Support Service Request

If the request or inquiry is accompanied by a priority level based on urgency and potential impact (Critical, High, Medium, Low), the Supplier shall meet the timeframes described below and adhere to all repair and warranty requirements in section 3) f) of this document.

  (a) **Critical:** This priority level consists of requests that are characterized as high urgency and high impact. Typically, these requests deal with issues that prevent the Authorized User from performing their primary work functions and have an enterprise/department/business unit-wide impact if unresolved. (These requests are most likely related to Core system issues)
  (b) **High:** This priority level consists of requests that are characterized as medium or moderate urgency and impact. Typically, these requests deal with issues that result in impaired work functions and have a business unit/user group impact.
  (c) **Medium:** This priority level consists of requests that are characterized as medium or moderate urgency and impact. Typically, these requests deal with issues that result in impaired/limited work functions but have an effect limited to a user group or a single user.
  (d) **Low:** This priority level consists of requests that are characterized as inconvenient. Typically, these requests are not crucial to primary business/operating functions.
  (e) Response time:
    (i) Critical: Instantaneous.
    (ii) High: 0-4 hours.
    (iii) Medium: Within 48 hours, (Two (2) business days).
    (iv) Low: Within five (5) business days.

Incident Response (IR)

It is very important for the State to have a detailed, clear, and effective understanding of the Supplier's incident response policy as well as redundancy and business continuity plans.

At a minimum, the support should include:

ii) Incident Response Requirements
  (1) Incident Response Detection Details
  (2) Security Incident Reporting and Notification Details
  (3) Data Breach Reporting Details
  (4) Redundancy and Business continuity details
  (5) Identify any known circumstances where a vulnerability in any of your products has resulted in a data breach for an end user within the past 5 years.
  (6) Safeguards that are in place to prevent unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of government information.
  (7) 24/7/365 Incident Response Services Details (24 hours per day, 7 days per week, 365 days out of the year support. Constantly, without interruption, twenty-four seven, the entire year.)
  (8) Single point of contact for incidents.
    (a) Supplier's assigned local account manager or TAM may not be the first to respond but should handle the logistics and resolution details of the incident once involved.
  (9) Root Cause Analysis (RCA) Requirements
    (a) Timing and Reporting: Supplier shall specify the timeframe within which the RCA report should be completed after the incident is resolved and establish the requirement for submitting the RCA report to Authorized User.
    (b) Scope and Depth: Supplier shall, in the RCA report, detail the root causes, contributing factors, and recommendations for corrective and preventive actions.
      (i) Corrective Actions: this should include the proactive steps to address the identified root causes and implement corrective actions promptly.
      (ii) Preventive Measures: Supplier shall propose preventive measures to avoid similar incidents in the future, based on the findings of the RCA.
  (10) Business Continuity, Disaster Recovery, and Geographic Redundancy Details
    (a) Supplier agrees to provide a network disaster recovery plan that outlines the procedures and strategies to recover and restore network operations in the event of a significant network failure or disaster.
      (i) Plan should include:
        1. Business continuity details
        2. A state/regional cloud network map for outage and redundancy purposes.
        3. Data backup strategy and plan
        4. Scenario options
        5. Temporary workaround details
        6. Disaster Testing

f) Repair and Warranty Requirements and Extended Warranty Offerings

Beyond the OEM standard warranty period, Suppliers should have robust repair and warranty offerings.

These repair and warranty offerings should meet or exceed the following:

i) Minimum and Extended Hardware Warranty
  (1) Supplier agrees that for a period of one (1) year of the date of purchase, hardware purchased by Authorized Users shall be free of defects in material and workmanship under normal authorized use consistent with the product instructions and specifications.
  (2) Supplier must repair or replace the warrantied equipment or provide a loaner or similar functionality for the Customer's use while replacement parts are located.

(3) Extended Warranty Offerings:
  (a) Supplier should offer Extended Warranty offerings at points of sale together with details of what each option include.

ii) Return Merchandise Authorization (RMA)

Suppliers should have a detailed and efficient RMA process that meets or exceeds the following:

(1) Supplier shall accept merchandise returns in re-sellable condition from Authorized Users for a period of thirty (30) calendar days after completion and acceptance of delivery. Supplier shall provide full credit or refund to Authorized Users, whichever an Authorized User requests, within thirty (30) calendar days on all returns that are in original packaging and in re-sellable condition.
(2) **Repair Process:** Supplier agrees to provide the process for requesting and obtaining repairs under the warranty. Including contact information for the warranty service provider or repair personnel. Details should include all the below items:
  (a) **Repair Specifications Details:** including any technical requirements, industry standards, and quality expectations.
  (b) **Warranty Period:** Specify the duration of the warranty for the repaired items or systems. This should state how long the warranty will be valid from the date of completion or acceptance.
  (c) **Warranty Coverage:** Clearly outline what is covered by the warranty and what is not. This may include parts, labor, transportation costs, and any limitations on the warranty.
  (d) **Exclusions and Limitations:** Mention any specific exclusions or limitations on the warranty coverage. For example, some warranties may not cover damage caused by misuse, accidents, or natural disasters.
  (e) **Quality Standards:** Quality standards for the repair work and compliance with relevant regulations and industry best practices.
  (f) **Reporting and Documentation:** Any detailed reports and documentation related to the repairs, warranty coverage, and maintenance activities.

(3) Dead on Arrival (DOA)
  (a) For hardware considered DOA Supplier will provide an expedited replacement within the first thirty (30) days from the shipment date of product from Supplier.
(4) Advanced RMA Options
  (a) Supplier shall provide details of any advanced RMA options available to Authorized Users.
    (i) This should include details around warehousing and any potential courier options available to Authorized Users.

iii) Software Warranty
(1) Supplier should provide details around their software warranty options. In addition, Supplier should also provide details regarding:
  (a) Software proprietary details.
    (i) Details around if the software is proprietary to a specific platform or specific equipment.
  (b) Software lifetime and end of support.
    (i) Minimum of one (1) year notification timeframe before software reaches end of support:

(c) Each year, during Authorized Users annual maintenance renewal window, Supplier should provide a technical roadmap of Supplier's software catalog, specifically related to Authorized Users current software infrastructure.
(i) End of support details
(ii) Replacement and upgrade options
(iii) Proprietary details

iv) Repair/Replacement time based on priority level:
(1) Critical: This priority level consists of requests that are characterized as high urgency and high impact. Typically, these requests deal with issues that prevent the Authorized User from performing their primary work functions and have an enterprise/department/business unit-wide effect if unresolved.
(2) High: This priority level consists of requests that are characterized as medium or moderate urgency and impact. Typically, these requests deal with issues that result in impaired work functions and have a business unit/user group impact.
(3) Medium: This priority level consists of requests that are characterized as medium or moderate urgency and impact. Typically, these requests deal with issues that result in impaired/limited work functions but have an effect limited to a user group or a single user.
(4) Low: This priority level consists of requests that are characterized as inconvenient. Typically, these requests are not crucial to primary business/operating functions.
(5) Repair/Replacement Time:
(a) Critical: Same business day.
(b) High: within one business day.
(c) Medium: within five (5) business days.
(d) Low: within ten (10) business days.

g) Networking Projects, Integrations, and Installations Procedures

i) Scope/Statement of Work (SOW)
(1) Supplier agrees that all Networking projects, integrations, and/or installations should be detailed and outlined using a comprehensive Scope/Statement of Work document (SOW). The comprehensive SOW should clearly state all necessary steps, goals, objectives, deliverables, requirements, constraints, and assumptions of the project and the process to fully achieve the Authorized User's project goals. The SOW should include, but not be limited to all deliverables, services, and written specifications that define the overall quality expectations, timeline, bill of materials or equipment listings, acceptance criteria, and any applicable drawings or diagrams specific to the project necessary for approval of payment.
(2) The SOW should be fully agreed upon by both the Authorized User and Supplier before the project can commence.

ii) Testing, Commissioning, and Acceptance
(1) The project/system must be fully tested by the Supplier with all possible sources and in every configuration prior to commissioning to the Authorized User.
(2) Acceptance testing, to ensure all of the acceptance criteria are met, is required for all networking projects, integrations, and/or installations before going live.
(3) Acceptance activities, applicable to each project, include but are not limited to, physical and mechanical inspections, operational tests, system testing, and individual item/equipment tests.
(4) At the conclusion of the acceptance testing, using the agreed upon SOW, the designee of the Authorized User and the Supplier shall jointly agree to the results of the testing, and reschedule testing on deficiencies and shortages, if any.

(5) Prior to project closeout, an inspection shall be performed to determine the completeness of the work. Projects cannot be signed off on until system functionality has been proven to meet project scope.
(6) After initial acceptance of networking project, integrations, and/or installation, Authorized User shall have the obligation to notify Supplier, in writing and within ten (10) days, or as otherwise agreed upon in the SOW, following provision of any deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a deliverable is unacceptable. Acceptance by Authorized User of any Supplier re-performance or correction shall not be unreasonably withheld but may be conditioned or delayed as required for confirmation by Authorized User that the issue(s) in the notice have been successfully corrected.

h) Data Security Standards and Requirements

The State desires for all State Agencies to have a comprehensive, best-in-class, structured data protection framework, where all networking equipment and any related software, is secure, efficient, compliant with all applicable industry security standards, applicable to the specific Agency's protected data. All laws, policies and standards are referenced with the intent of any updates to aforementioned be automatically incorporated by reference.

i) Supplier agrees to conform to the State IT Policies, Standards, and Procedures, including but limited to those which may be found at https://gta.georgia.gov/psg/ or a successor URL(s), and any applicable University System of Georgia (USG) Information Technology Standards and Procedures which may be found at https://www.usg.edu/information_technology_services/it_handbook/ or a successor URL(s), as are pertinent to Supplier's operation and provision of services and deliverables.
ii) Supplier shall not access Sensitive State Data, except as requested in writing, or permitted by Authorized user in the following scenarios:
    (1) during data center operations,
    (2) in response to service or technical issues,
    (3) as required by Supplier to perform the services covered by this Agreement or
    (4) at the State's request. Contractor has a limited, non-exclusive license to use Sensitive State Data solely for the purpose of performing its obligations under this Agreement. Storage of Sensitive State Data at rest shall be located solely in location(s) or data centers in the U.S., and Supplier shall notify State of such locations. Please refer to Attachment K. Statewide Contract for Networking Equipment & Related Services Attachment 4. Data Security Terms and Conditions for detailed requirements.
iii) Data Encryption: Supplier agrees that all sensitive data, both in transit and at rest, must be encrypted in accordance with State IT Policies, Standards, and Guidelines, https://gta.georgia.gov/psg/.
iv) Access Control: Supplier should implement strong access controls to ensure that only authorized personnel can access sensitive data. This may include role-based access control (RBAC) and multi-factor authentication (MFA).
v) Data Storage and Retention: Please refer to Attachment K. Statewide Contract for Networking Equipment & Related Services Attachment 4. Data Security Terms and Conditions for detailed requirements.
vi) Audit Logs: Supplier shall create and retain detailed audit logs that track user activities and access to sensitive data for monitoring and review purposes.
vii) Security Testing and Auditing: Supplier shall provide information and details regarding regular security testing, vulnerability assessments, and penetration testing to identify and address potential weaknesses in the data security infrastructure.

(1) **In accordance with Attachment K. Statewide Contract for Networking Equipment and Services v2, Attachment 4, section V. A. Data Center Audit, if selected for contract award, Supplier shall provide DOAS with a copy of a third-party audit report of the Supplier's security controls on an annual basis. Supplier must submit the report within 30 days upon request. The audit report must be on the security controls currently used by the OEM.**

viii) Security Incident Response: Supplier shall provide an effective incident response plan, outlining procedures for identifying, containing, and mitigating data breaches or security incidents.

ix) Data Breach Notification: Supplier must promptly notify Authorized User in the event of a data breach and provide detailed information about the incident, including affected data and mitigation steps taken. Please refer to Attachment K. Statewide Contract for Networking Equipment & Related Services Attachment 4. Data Security Terms and Conditions for detailed requirements.

x) Secure Development Practices: Supplier agrees to adhere to secure coding practices during the development of software or applications that handle sensitive data.

xi) Physical Security: Please refer to Attachment K. Statewide Contract for Networking Equipment & Related Services Attachment 4. Data Security Terms and Conditions for detailed requirements.

xii) Data Privacy Compliance: Supplier agrees to comply with all relevant data privacy laws and regulations.

xiii) Employee Training and Awareness: Supplier should have an employee data security training program and should provide details of its data security training programs for employees to ensure they are aware of best practices and potential risks.

xiv) Third-Party Security Assessments: Supplier agrees that all third-party services or subprocessors, should conduct security assessments to ensure data protection throughout the supply chain.

xv) Data Backup and Disaster Recovery: Supplier should have should haver data backup procedures and disaster recovery plans to ensure data availability and continuity in the event of a catastrophic incident.

xvi) Network Security: Supplier should have security measures to protect network infrastructure, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

xvii) In addition to Supplier agreeing to conform to the State IT Policies, Standards, and Procedures mentioned in subsection i) of this section, if applicable according to the needs of the purchasing entity identified at the point of sale, Supplier and its Authorized Servicing partners agree comply with all the below security standards:

NIST CSF	National Institute of Standards and Technology Cyber Security Framework	The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.
NIST 800-171	National Institute of Standards and Technology Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations
CMMC	Cybersecurity Maturity Model Certification	Protect sensitive defense information from cyber-attacks and nation state actors. Create a unifying cybersecurity standard for defense contractors. Ensure accountability for defense companies that are responsible for protecting

		government data. CMMC is required of any individual in the DOD supply chain, including contractors who interact exclusively with the Department of Defense and all subcontractors.
FIPS	Federal information processing standards	The Federal Information Processing Standards (FIPS) of the United States are a set of publicly announced standards that the National Institute of Standards and Technology (NIST) has developed for use in computer systems of non-military, American government agencies and contractors.

4) Optional Services

a) Leasing or Alternative Financing Methods

i) The use of leasing or alternative financing methods for the acquisition of equipment, products, and services under this contract is permitted.

ii) It is not a requirement where a Supplier must be able to offer leasing or alternative financing methods.

iii) If Supplier can offer leasing or alternative financing methods, the negotiated Leasing/Finance agreement, should be the only Leasing/Finance agreement in place governing all the Leasing/Financing purchases by Authorized Users of the State. The agreement should be static and should not include any hyperlinks to any other Supplier-related terms and conditions.

Category 1: Core Networking & Infrastructure Products Cost Workbook

Juniper Networks

Please Note: All Yellow Highlighted Cells Require Supplier Input

CATEGORY DISCOUNT SUMMARY TABLE	SUPPLIER PROPOSED MINIMUM DISCOUNT % OFF	SUPPLIER PROPOSED MINIMUM EDUCATIONAL DISCOUNT % OFF
Core Products / Equipment / Hardware Discount	45%	49%
Product / Hardware Maintenance Licensing & Support Discount	15%	17%
Software / Subscription Discount	45%	49%

PRODUCTS (EQUIPMENT/HARDWARE OR SOFTWARE/CLOUD SOLUTION)								SUPPLIER PROPOSED MINIMUM DISCOUNT % OFF:	SUPPLIER PROPOSED MINIMUM EDUCATIONAL DISCOUNT % OFF:
								45%	49%
PRODUCT SPECIFICATION:				SUPPLIER PROPOSED:					
LINE ITEM #	TYPE	MINIMUM SPECIFICATIONS REQUIRED	UOM (UNIT OF MEASURE)	MANUFACTURER NAME OR BRAND NAME	PART/MODEL #	NATIONALLY PUBLISHED MSRP PER UOM	INITIAL YEAR TOTAL COST OF OWNERSHIP PER UOM	EVALUATED COST PER UOM	EVALUATED COST PER UOM
1	Campus LAN - Access Switch	Provides initial connectivity for devices to the network and controls user and workgroup access to internetwork resources. Features a campus LAN access switch should support: 1. Security a. SSHv2 b. 802.1X (Port Based Network Access Control) c. Port Security d. DHCP Snooping 2. VLANs 3. Fast Ethernet/Gigabit Ethernet 4. PoE (Power over Ethernet) 5. link aggregation 6. 10 Gb support 7. Port mirroring/Span Taps 8. Support of IPv6 and IPv4 9. Standards-based rapid spanning tree 10. Netflow/Sflow Support 11. Layer 2 and/or layer 3	EACH	Juniper	EX2300-24P	$ 3,232.00	$ 3,717.00	$ 1,937.65	$ 1,796.73
LINE ITEM #	TOTAL COST OF OWNERSHIP INCLUDES:	DEFINITION:		DESCRIPTION:			PRICE PER YEAR OF TCO	TOTAL EVALUATED COST	
1A	Additional Items for full functionality of product and total cost of ownership for five years.	The State needs full transparency and insight into how the pricing structure of goods and services is determined and strategically planned regarding the life cycle of the goods and services offered by the Supplier. This includes understanding what additional items are included in a purchase for the products to be fully functional. Please provide all additional items, (maintenance license, firmware updates, software, support, etc.) for this product SKU to be fully functional and operational to its full capacity for five (5) years. (If the cost of the additional items are already included in the initial product cost, please enter $0.00 for these items)						$ 1,843.23	
	Year 1			Supplier annual functionality details here.			$ 97.00		
	Year 2			Supplier annual functionality details here.			$ 97.00		
	Year 3			Supplier annual functionality details here.			$ 97.00		
	Year 4			Supplier annual functionality details here.			$ 97.00		

	Year 5			Supplier annual functionality details here.			$ 97.00		
LINE ITEM #	**TYPE**	**MINIMUM SPECIFICATIONS REQUIRED**	**UOM (UNIT OF MEASURE)**	**MANUFACTURER NAME OR BRAND NAME**	**PART/MODEL #**	**NATIONALLY PUBLISHED MSRP PER UOM**	**INITIAL YEAR TOTAL COST OF OWNERSHIP PER UOM**	**EVALUATED COST PER UOM**	**EVALUATED COST PER UOM**
2	Core / Edge Routers	High performance, high speed, low latency routers that enable Enterprises to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV and Video on Demand, and Software as a Service	EACH	JUNIPER	MX204-HW-BASE	$ 40,500.00	**$ 48,155.00**	**$ 24,801.15**	**$ 22,997.43**
LINE ITEM #	**TOTAL COST OF OWNERSHIP INCLUDES:**	**DEFINITION:**		**DESCRIPTION:**			**PRICE PER YEAR OF TCO**	**TOTAL EVALUATED COST**	
2A	Additional Items for full functionality of product and total cost of ownership for five years.	The State needs full transparency and insight into how the pricing structure of goods and services is determined and strategically planned regarding the life cycle of the goods and services offered by the Supplier. This includes understanding what additional items are included in a purchase for the products to be fully functional. Please provide all additional items, (maintenance license, firmware updates, software, support, etc.) for this product SKU to be fully functional and operational to its full capacity for five (5) years. (If the cost of the additional items are already included in the initial product cost, please enter $0.00 for these items)						**$ 23,592.66**	
	Year 1			Supplier annual functionality details here.			$ 1,531.00		
	Year 2			Supplier annual functionality details here.			$ 1,531.00		
	Year 3			Supplier annual functionality details here.			$ 1,531.00		
	Year 4			Supplier annual functionality details here.			$ 1,531.00		
	Year 5			Supplier annual functionality details here.			$ 1,531.00		
LINE ITEM #	**TYPE**	**MINIMUM SPECIFICATIONS REQUIRED**	**UOM (UNIT OF MEASURE)**	**MANUFACTURER NAME OR BRAND NAME**	**PART/MODEL #**	**NATIONALLY PUBLISHED MSRP PER UOM**	**INITIAL YEAR TOTAL COST OF OWNERSHIP PER UOM**	**EVALUATED COST PER UOM**	**EVALUATED COST PER UOM**
3	Wireless Access Points - Indoor	A wireless Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. Capabilities should include: • 802.11a/b/g/n • 802.11n • 802.11ac • Centralized management capabilities • UL2043 plenum rated for safe mounting in a variety of indoor environments • Support AES-CCMP (128-bit) • Provides real-time wireless intrusion monitoring and detection	EACH	Juniper/Mist	MIST-AP32-1S-5Y	$ 1,751.00	**$ 1,751.00**	**$ 963.05**	**$ 893.01**
LINE ITEM #	**TOTAL COST OF OWNERSHIP INCLUDES:**	**DEFINITION:**		**DESCRIPTION:**			**PRICE PER ITEM IN TCO**	**TOTAL EVALUATED COST**	
3A	Additional Items for full functionality of product and total cost of ownership for five years.	The State needs full transparency and insight into how the pricing structure of goods and services is determined and strategically planned regarding the life cycle of the goods and services offered by the Supplier. This includes understanding what additional items are included in a purchase for the products to be fully functional. Please provide all additional items, (maintenance license, firmware updates, software, support, etc.) for this product SKU to be fully functional and operational to its full capacity for five (5) years. (If the cost of the additional items are already included in the initial product cost, please enter $0.00 for these items)						**$ 916.12**	
	Year 1			Supplier annual functionality details here.			$ -		
	Year 2			Supplier annual functionality details here.			$ -		
	Year 3			Supplier annual functionality details here.			$ -		

	Year 4			Supplier annual functionality details here.			$ -		
	Year 5			Supplier annual functionality details here.			$ -		
LINE ITEM #	**TYPE**	**MINIMUM SPECIFICATIONS REQUIRED**	**UOM (UNIT OF MEASURE)**	**MANUFACTURER NAME OR BRAND NAME**	**PART/MODEL #**	**NATIONALLY PUBLISHED MSRP PER UOM**	**INITIAL YEAR TOTAL COST OF OWNERSHIP PER UOM**	**EVALUATED COST PER UOM**	**EVALUATED COST PER UOM**
4	Wireless Access Points - Outdoor	Outdoor access points work similarly to indoor access points, but support higher power levels and have purpose-built antennas. They rely on dedicated radios to connect client and IoT devices over a WLAN. Most also include radios to support IoT, including low- or high-powered Bluetooth and Zigbee. Unlike indoor access points, they are waterproof and temperature hardened to better support challenging industrial IoT and manufacturing environments which include built-in antenna options and protected power options to provide full coverage in any weather. An outdoor wireless access point is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. Capabilities should include: • 802.11a/b/g/n • 802.11n • 802.11ac • Centralized management capabilities • Outdoor Mounting • IP Rating (IP66 or IP67) • Antenna Option (Omni, Directional, or External Option) • Support AES-CCMP (128-bit) • Provides real-time wireless intrusion monitoring and detection	EACH	Juniper/Mist	MIST-AP63-1S-5Y	$ 3,349.00	**$ 3,349.00**	**$ 1,841.95**	**$ 1,707.99**
LINE ITEM #	**TOTAL COST OF OWNERSHIP INCLUDES:**	**DEFINITION:**		**DESCRIPTION:**			**PRICE PER ITEM IN TCO**	**TOTAL EVALUATED COST**	
4A	Additional Items for full functionality of product and total cost of ownership for five years.	The State needs full transparency and insight into how the pricing structure of goods and services is determined and strategically planned regarding the life cycle of the goods and services offered by the Supplier. This includes understanding what additional items are included in a purchase for the products to be fully functional. Please provide all additional items, (maintenance license, firmware updates, software, support, etc.) for this product SKU to be fully functional and operational to its full capacity for five (5) years. (If the cost of the additional items are already included in the initial product cost, please enter $0.00 for these items)						**$ 1,752.20**	
	Year 1			Supplier annual functionality details here.			$ -		
	Year 2			Supplier annual functionality details here.			$ -		
	Year 3			Supplier annual functionality details here.			$ -		
	Year 4			Supplier annual functionality details here.			$ -		
	Year 5			Supplier annual functionality details here.			$ -		
LINE ITEM #	**TYPE**	**MINIMUM SPECIFICATIONS REQUIRED**	**UOM (UNIT OF MEASURE)**	**MANUFACTURER NAME OR BRAND NAME**	**PART/MODEL #**	**NATIONALLY PUBLISHED MSRP PER UOM**	**INITIAL YEAR TOTAL COST OF OWNERSHIP PER UOM**	**EVALUATED COST PER UOM**	**EVALUATED COST PER UOM**
5	Wireless Controller / Management	An onsite or offsite solution utilized to manage Light-weight access points in large quantities by the network administrator or network operations center. The WLAN controller automatically handles the configuration of wireless access-points. Capabilities should include: • Ability to monitor and mitigate RF interference/self-heal • Support seamless roaming from AP to AP without requiring re-authentication • Support configurable access control lists to filter traffic and denying wireless peer to peer traffic • System encrypts all management layer traffic and passes it through a secure tunnel • Policy management of users and devices provides ability to de-authorize or deny devices without denying the credentials of the user, nor disrupting other AP traffic	EACH	Juniper/Mist	ME-X1	$ 12,815.00	**$ 19,380.00**	**$ 9,214.70**	**$ 8,544.54**
LINE ITEM #	**TOTAL COST OF OWNERSHIP INCLUDES:**	**DEFINITION:**		**DESCRIPTION:**			**PRICE PER ITEM IN TCO**	**TOTAL EVALUATED COST**	

5A	Additional Items for full functionality of product and total cost of ownership for five years.	The State needs full transparency and insight into how the pricing structure of goods and services is determined and strategically planned regarding the life cycle of the goods and services offered by the Supplier. This includes understanding what additional items are included in a purchase for the products to be fully functional. Please provide all additional items, (maintenance license, firmware updates, software, support, etc.) for this product SKU to be fully functional and operational to its full capacity for five (5) years. (If the cost of the additional items are already included in the initial product cost, please enter $0.00 for these items)			$ 8,765.69
	Year 1		Supplier annual functionality details here.	$ 1,313.00	
	Year 2		Supplier annual functionality details here.	$ 1,313.00	
	Year 3		Supplier annual functionality details here.	$ 1,313.00	
	Year 4		Supplier annual functionality details here.	$ 1,313.00	
	Year 5		Supplier annual functionality details here.	$ 1,313.00	
					$ 36,869.90

Partner Name	Sales Contact	Sales Contact Email	Sales Contact Tele	Address	City, State, Zip	Web Site
Ansley Communications DBA ACG Solutions	Charles Ansley	cansley@ansleycomm.c	(770) 771-6159	1058 W. Airport Rd.	Cornelia Ga. 30531	https://www.acg-solutions.com/
BlueAlly Technology Solutions LLC	Monica Davis	mdavis@blueally.com	(404) 316-3565	1225 Cresecent Green Suite 115	Cary, NC 27518	BlueAlly | Conquer IT complexity
Converged Networks LLC	Michael Hauer	mhauer@convergednet	(843) 725-3200	2 Still Shadow Drive, Suite G	Charleston, SC 29414	www.convergednetworks.com
ConvergeOne, Inc.	Liz Schweitzer	lschweitzer@onec1.con	(314) 594-1231	10900 Nesbitt Avenue S	Bloomington, MN 55437	https://www.onec1.com/
Data Network Solutions, Inc	Kin Wong	kwong@datanetworkso	(803) 932-9914	629 Lake Tide Dr	Chapin, SC 29036	www.datanetworksolutions.com
Encore Technology Group, LLC	Morgan Love	mlove@encoretg.com	(770) 666-1433	202 Wall Street	Piedmont, SC 29673	www.encoretg.com
ITsavvy LLC	Emilio Leath	eleath@ITsavvy.com	(630) 396.6379	2015 Spring Road, Suite 300	Oak Brook, IL 60523	www.ITsavvy.com
Kopesky Enterprises Inc, DBA SureLock Technology	Bob Kopesky	bkopesky@surelocktech	(678) 712-5346	4908 Golden Parkway Suite 800	Buford, GA 30518	surelocktechnology.com
Kopesky Enterprises Inc, DBA SureLock Technology	Scott Mathewson	smathewson@surelockt	(706) 775-8345	4908 Golden Parkway Suite 800	Buford, GA 30518	surelocktechnology.com
Network Technology Solutions, LLC	Sam Reynolds	sam.reynolds@network	(229) 226-2110	138 S. Madison Street	Thomasville, GA 31792	www.ntsnetworks.com
NTT America, Inc.	Julie Campbell	julie.campbell@global.r	(775) 737-1939	One Penn Plaza, Suite 4920	New York, NY 10119	https://services.global.ntt/en-us/
PC Solutions and Integration, Inc.	Katie Simpson	ksimpson@pcsusa.net	706-499-5583	668 South Main Street	Cornelia, GA 30531	www.pcsusa.net
PC Solutions and Integration, Inc.	Kendra Kull	kkull@pcsusa.net	954-270-1030	668 South Main Street	Cornelia, GA 30531	www.pcsusa.net
Presidio Networked Solutions LLC	Catherine Bowen	cbowen@presidio.com	(404) 381-1418	3340 Peachtree Rd., Suite 2700	Atlanta, GA 30326	www.presidio.com
United Data Technologies, Inc. d/b/a UDT	Logan Sevier	lsevier@udtonline.com	(912) 373-5520	2900 Monarch Lakes Boulevard, Suite 300	Miramar, FL 33027	udtonline.com
MGT Impact Solutions, LLC	Scott Faxon	sfaxon@mgt.us	770-225-5300	1450 Oakbrook Dr Ste 900	Norcross, GA 30093-6239	www.mgt.us