AMENDMENT TWO
STATE TERM CONTRACT 204X
(IFB ITS-400277)

THIS AMENDMENT 2 is entered into by and between North Carolina Department of Information Technology ("DIT"), 3700 Wake Forest Road, Raleigh, NC 27609, and Cisco Systems, Inc. ("Cisco"), 170 W. Tasman Drive, San Jose, CA 95134 ("Vendor").

The parties acknowledge they entered into a contract, IFB ITS-400277, in April 2019 to provide Cisco server, storage, and networking equipment, maintenance, and related professional services to the State of North Carolina. The contract was amended in May 2019 (Amendment 1) to correct a pricing error with the Minimum Percentage off List Discounts in Cisco Best and Final Offer Response to IFB ITS-400277(AGREEMENT).

The parties now wish to amend the Agreement as follows:

1) Add the following Cisco Cloud and SaaS product offerings (Licensor's Agreement) to the 204X Agreement (Exhibit A):
   - Cisco Universal Cloud Agreement (as modified herein)
   - Cisco Tetration Supplemental End User License Agreement and Cisco Tetration SaaS Offer Description (as modified herein)
   - Cisco AnyConnect Supplemental End User License Agreement
   - Cisco Intersight Offer Description
   - Cisco AppDynamics Offer Description (as modified herein)

2) The Licensor's Agreement is modified by this Amendment, and therefore, conflicts arising among the terms of the Licensor's Agreement and the terms of this Amendment shall be resolved by the following order of precedence:
   a) This Amendment,
   b) BAFO ITS-400277
   c) IFB ITS-400277 not superseded by the BAFO
   d) The Licensor's Agreement,
   e) Terms and other documents incorporated by reference in the Licensor's Agreement.

3) General modifications to the Cisco Licensor's Agreement:

   a) Notwithstanding terms and conditions, hyperlinks, or similar references to additional license agreements of third Parties presented in Licensor's Agreement, the State shall not be obligated under the Licensor's Agreement, or other agreements, to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, legal fees, termination costs, costs of audits, or other similar costs.

   b) Third Party Software, Open Source Software, and flow down terms: Notwithstanding terms and conditions, hyperlinks, or similar references to additional license agreements of third Parties presented in Licensor's Agreement, the State has no financial obligation or liability to Vendor or such third parties under such additional license agreements. The State will not knowingly violate the licensing limitations stated in such additional license agreements.

c) Clickwrap / universal license by use or installation: Notwithstanding terms of the Licensor's Agreement conditioning the license grant upon acceptance of terms when downloading, installing, using, etc. the software (e.g. by using the software, you accept and agree to the terms and conditions of this agreement), such conditions shall not bind the State or its agencies, and such conditions shall be superseded by this Amendment to the License Agreement.

d) Notwithstanding any payment terms in the Licensor's Agreement, the State's payment obligations pursuant to the 204X contract (IFB ITS-400277) shall supersede the payment terms in the Licensor's Agreement, and the State shall have no payment obligation to Licensor pursuant to the payment terms in the Licensor's Agreement.

e) **SECURITY OF STATE DATA:**

Definitions: The following are additional defined terms:

Administrative Data: means information collected by Cisco related to the State's contracting, registration, ordering and invoicing process with Cisco, or requests for information from the State on Cisco's offerings.

Cybersecurity Incident: An occurrence that:

a. Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.

Data: includes information, formulae, algorithms, metadata, instruments, studies, reports, records and other materials or content that the State, the State's employees, agents and end users upload, create or modify using the Services under this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable. Administrative Data, Support Data, and Telemetry Data will not be considered Data.

Security Breach: means a Security Breach as defined within N.C.G.S. § 75-61.

Significant Cybersecurity Incident: A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:

1. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or

2. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

b. Incidents that involve information that is not recoverable or cannot be recovered within defined time lines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through

additional measures and has a high or medium functional impact to the mission of an agency.

Support Data: means information that Cisco collects when the State submits a request for support services or other troubleshooting.

Telemetry Data: means information and data that Cisco's product or service generates or derives in connection with the State's use of the product or service.

1. All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State pursuant to the Vendor Licensor Agreements. The Vendor will implement measures designed to protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as necessary for the performance or provision of Services or as required by the express terms of this contract, or (iv) at State's written request.
2. Vendor shall implement measures designed to protect the confidentiality of all Data provided to it by the State or maintained or created in accordance with this Agreement. No such Data in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State, except to Vendor affiliates and subcontractors, only as necessary for the performance or provision of Services. The Vendor will have written policies generally governing data protection policies and standards.
3. Vendor agrees that it shall not store or transfer non-public State data outside of the United States for Vendor's offers listed under Section 2, Exhibit A. This includes backup data and Disaster Recovery locations. All other Vendor offers shall be restricted to public State data only as noted under Section 3, Exhibit A. The Vendor will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
4. Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing, in accordance with its information security policies, any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (https://it.nc.gov/document/statewide-data-classification-and-handling-policy), that is collected or uploaded, in accordance with the Vendor License Agreements, by the State into any Vendor offering and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor agrees, at its sole cost and expense, that it shall implement processes designed to maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident impacting State data within 24 hours of confirmation as required by N.C.G.S. § 143B-1379. Vendor shall send notifications of such Security Breaches,

Cybersecurity Incident or Significant Cybersecurity Incident notifications to the following:

State Enterprise and Security Risk Management Office:
Email: dit.threatmanagement@nc.gov (Mon. – Fri.; 8:00 am – 5:00 pm)
After Hours: soc@nc.gov
DIT Service Desk: 919-754-6000 or 800-722-3946

5. If such functionality is included in the Vendor offering and purchased by the State, Vendor will provide and maintain secure backup of the State Data. Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement designed to secure such Data from a Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident and protect the Data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
6. Vendor shall certify to the State:
    i. Upon request and on an annual basis, during the term of the contract and subject to obligations of confidentiality, the sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
    ii. If the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the Vendor's data classification level and security controls. The State reserves the right to independently evaluate, audit, and verify such requirements according to the due diligence questionnaire and audit terms established herein. Vendor shall develop and maintain documentation to demonstrate its alignment with relevant industry standards (such as ISO and NIST) and standards required by this Agreement. The State may verify Vendor's compliance by having the Vendor complete a due diligence questionnaire, not more than once annually. If Vendor has not provided satisfactory answers within sixty (60) days, or if the State still has reasonable and specific grounds to suspect non-compliance after provision of responses, the State may request an on-site audit (at the State's cost), not more than once every 12 months. The Vendor's AppDynamics offer is excluded from the on-site audit provision. If the State exercises such right, the State will use a mutually acceptable independent third party auditor. To request an audit, the State will submit a detailed proposed audit plan to the Vendor. The proposed audit plan will describe the proposed scope, manner, duration, and start date of the audit. The Vendor will review the proposed audit plan and provide any concerns or questions (for example, any request for information that could compromise the Vendor's security, privacy, employment or other relevant policies). The Vendor and State will then mutually agree upon an audit date and location. The audit will be conducted during regular business hours at the agreed facility, subject to the agreed final audit plan and the Vendor's

health and safety or other relevant policies, and may not unreasonably interfere with the Vendor's business activities. The Vendor will address, in a timely manner, any security issues that are uncovered in such assessments. Nothing herein shall be construed as a derogation of the State Auditor's authority or the State CIO's authority as granted by NCGS §§ 147-64.7(a) and 143B-1378, respectively.

iii. That the Services will comply with the following:

1) Upon request, Vendor shall provide a completed Vendor Readiness Assessment Report ("VRAR") for Non-State Hosted Solutions that are included in the contract. This report is located at the following website: https://it.nc.gov/documents/vendor-readiness-assessment-report-vrar. The State will review the VRAR for security and privacy requirements in compliance with the Statewide Information Security Manual. The Vendor must meet or exceed the requirements identified in the VRAR.
2) Encryption requirements as defined below:
    a. The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
    b. For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest except as otherwise provided herein. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Vendor does not offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach as provided in Exhibit A, Paragraph 1. Additionally, where encryption of sensitive personally identifiable data at rest is not offered by the Vendor, the Vendor must describe existing security measures that provide analogous protection.
3) Applicable Federal and State laws including but not limited to the Federal Privacy Act of 1974, North Carolina Identity Theft Protection Act, North Carolina Public Records Act, N.C.G.S. Chapter 132 and
4) The Vendor's Information Security Program is modeled leveraging industry standards, such as ISO 27001 or NIST standards.

7. Breach Notification. In the event Vendor becomes aware of any Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) notify the State's Chief Risk Officer of such Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident within 24 hours of confirmation, (2) investigate such Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident, (3) provide a mutually acceptable remediation plan, acceptance of which shall not be unreasonably withheld by the State, to address the Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident and

prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, or other duly authorized representative of the State investigating such Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident. The State shall make the final decision on the implementation of any portion of the remediation plan that requires State action. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

8. Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such confirmed Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external ~~actual~~ costs associated with addressing and responding to the Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. In the event that Vendor becomes aware of any Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
9. After a Security Breach, Cybersecurity Incident or Significant Cybersecurity Incident, Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and are directly related to the State's Data, at no cost to the State.
10. In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
11. In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data as may be set forth in any agreed upon or applicable SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss

of access may result in the State exercising its options for assessing damages under this Agreement.

12. In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the affected State Agency and, to the extent the State has provided its preferred contact method, the State Chief Information Officer or designee of the contracting agency. Each agency purchasing pursuant to this Agreement will provide written notice to Vendor identifying its contact person(s) by name, role or position and contact information to enable delivery of notification(s) pursuant to this Paragraph. Vendor shall provide such notification within twenty-four (24) hours after Vendor confirms there has been such a disaster or catastrophic failure. In the notification, to the extent the following information is available, Vendor shall inform the State of the information listed below. To the extent the following information is not available at the time of the initial Vendor notification to the State, the Vendor agrees to provide the information, and updates to such information, to the State when it becomes available.
    1) The scale and quantity of the State Data loss;
    2) What Vendor has done or will do to recover the State Data from backups if data backups is included in the Vendor offering and is purchased by the State and mitigate any deleterious effect of the State Data and Services loss; and
    3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
    4) If Vendor fails to respond immediately and remedy the failure in accordance with Vendor's Business Continuity and Disaster Recovery Plan, the State may exercise its options for assessing damages or other remedies available under this Agreement.

    Vendor shall conduct an investigation of the disaster or catastrophic failure and shall, upon request, share information with the State pertaining to the State's Data loss, extended loss of access to Data, or Services. The State (at its expense) and/or its authorized agents shall have the right to lead (if required by law) or participate in an investigation of such loss. Vendor shall cooperate with the State, its agents and law enforcement of any such investigation.
13. In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph m, Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and/or convert the State Data.
14. Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested Data in all of its forms except to the extent Vendor is required by applicable law to retain some or all of the data (in which case Vendor will archive the data and implement reasonable measures to prevent the data from any further processing), for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of

Standards and Technology (NIST) approved methods, and certificates of destruction shall be provided to the State upon request.

f) Notwithstanding any terms and conditions in the Licensor's Agreement regarding data collection, storage, and/or processing, the Customer shall permit the Vendor to access or temporarily retain information necessary to perform the Services. ~~Customer may, in its discretion, disallow retainage of any information outside of the U.S~~. To temporarily retain, as used herein, shall mean to retain for only such time as necessary to perform tasks for the Customer and with the Customer's concurrence.

4) The following modifications are made to the Cisco Universal Cloud Agreement where "reserved" removes such a term as void:

a) Section 2 "Your Payment Obligations" is modified as follows:

~~Fees for the Cloud Service set out in Your purchase terms with Your Approved Source are non-refundable and payment obligations are non-cancelable, except as provided herein, in those purchase terms or where prohibited by law.~~ If Your use of the Cloud Service(s) exceeds Your entitlement rights, You agree to pay for Your excess use as required under Your purchase terms or Cisco buying program.

b) Section 3 "Your Use of the Cloud Service", paragraph c "Use in China or Russia" is reserved.
c) Section 3 "Your Use of the Cloud Service", paragraph d "Use by Authorized Users" is modified as follows:

1. You may allow third parties to use the Cloud Service solely on Your behalf for Your internal operations. You are responsible for ensuring that all Authorized Users comply with the terms of this Agreement.~~ and You are liable for any breach of this Agreement by Your Authorized Users. If You have purchased the Cloud Service under a Cisco buying program, further restrictions may apply. To the extent permitted by applicable law, You must ensure that third parties using the Cloud Service on Your behalf bring all claims related to the Cloud Service through You and waive all claims directly against Cisco related to those claims.~~

d) Section 3 "Your Use of the Cloud Service", paragraph e "Third Party Products" is clarified as follows:

1. "Third party products" is limited to non-Cisco products that are not procured under this, or any other, agreement between the State and Cisco.

e) Section 4 "Confidential Information and Data", paragraph a "Confidential Information" is reserved.
f) Section 4 "Confidential Information and Data", paragraph d "International Data Transfers" is reserved.
g) Section 5 "Ownership and Software Licensing Rights", paragraph a "What You Own" is modified as follows:

1. You retain ownership in all intellectual property rights to Your Customer Data. You authorize Cisco to use non-confidential feedback and ideas You provide in connection with Your use of the Cloud Service is limited to providing the contracted

service, improving contracted services.

h) Section 6 “Indemnification” is reserved in its entirety.

i) Section 7 “Warranties, Disclaimers and Limitation of Liability”, paragraph c “Limitation of Liability” is reserved.

j) Section 8 “Term and Termination”, paragraph b “Renewal” is modified as follows:

~~In order to provide You with uninterrupted service, the Cloud Service will automatically renew for the renewal period selected on the Order (“Renewal Term”) unless: (i) You notify the Approved Source in writing at least thirty (30) days before the end of the then-current term of Your intention not to renew; or (ii) You or Your Approved Source elect on the Order at the time of initial purchase not to auto-renew the Cloud Service; or (iii) the end-of-sale date for the Cloud Service has passed.~~ Your Approved Source will notify You reasonably in advance of any Renewal Term if there are any fee changes. The new fees will apply for the upcoming Renewal Term unless You notify the Approved Source in writing before the applicable renewal date that You do not accept the fee changes. In such event, the Cloud Service will terminate at the end of the then-current term.

k) Section 8 “Term and Termination”, paragraph c “Termination” is modified as follows:

If a party materially breaches this Agreement and does not cure that breach within thirty (30) days after receipt of written notice of the breach, the non-breaching party may terminate this Agreement for cause. Cisco also has the right to immediately suspend or terminate Your use of the Cloud Services if You breach Sections 3a, 5c ~~or 9e~~. Upon termination or expiration of this Agreement, You must cease any further use of the Cloud Service (and destroy any copies of Software within Your control). Upon any termination for Cisco’s material breach of the Agreement, we will refund to You or Your Approved Source any prepaid fees covering the period from the effective date of termination to the end of the term. Upon Cisco’s termination for Your material breach of the Agreement, You will pay any unpaid fees covering the period ~~from the~~ up to the effective date of termination ~~to the end of the term~~.

l) Section 8 “Term and Termination”, paragraph e “Survival” is modified as follows:

The following sections survive the expiration or termination of this Agreement: 2 (as modified herein), 3a, 3b, & 3d-3e (as modified herein), 4b, 4c, 5a (as modified herein), 5b, the last sentence of 5c, 7a, 7b, 9a, 9c, 9d, 9e, 9f, 9h, 9i (as modified herein), and 9k.

m) Section 9 “General Provisions”, the following paragraphs are reserved:

- Paragraph b “Modifications to the Agreement”
- Paragraph g “Governing Law and Venue”
- Paragraph j “Force Majeure”
- Paragraph l “Integration”

n) Section 9 “General Provisions”, paragraph i “Notification” is modified as follows:

Cisco may provide You with notice via email, regular mail ~~and/or postings on the Cisco.com website or any other website used as part of the Cloud Service~~. Notices to Cisco should be sent to Cisco Systems, Office of General Counsel, 170 Tasman Drive, San Jose, CA 95134 unless an applicable Offer Description specifically allows other means of notice.

o) Section 10 “Definitions”, paragraph “Confidential Information,” is reserved.

5) The following modification is made to the Offer Description: Cisco Tetration SaaS:

a) Paragraph entitled “Supplemental Terms and Conditions” is modified as follows: Tetration includes “Tetration APIs” and “Tetration Apps,” additional functionality subject to these additional terms, which you agree to if you use either of them. You are licensed to use and make calls to the Tetration APIs and Tetration Apps for the sole purpose of developing and implementing software applications that work, communicate, or interact with Your licensed Tetration products. You agree not to develop intellectual property with use of and/or used with the Tetration APIs or Tetration Apps and therefore will not have standing to assert intellectual property rights against Cisco or any of its affiliates, customers, resellers, distributors, or other licensees of the Tetration APIs and Tetration Apps for making, having made, using, selling, offering for sale, or importing: (i) any products or services implementing, interfacing with or operating in combination with the Tetration APIs or Tetration Apps; or (ii) any applications developed using the Tetration APIs or Tetration Apps. If You do not agree with the foregoing terms for Tetration APIs and Tetration Apps, do not make use of such functionality.

6) The following modifications are made to the Offer Description: AppDynamics:

a) Paragraph 1 “Overview” is modified to strike the following sentence: “With respect to this Offer Description, the following section of the UCA is not applicable to Your use of the Software: 5(c) (Software License & Restrictions)”.

b) Paragraph 2.B “Services” is modified as follows: “If AppDynamics is unable to reallocate such resources AppDynamics may deduct from Your pre- paid Services (or You will pay for) the amount of Services that were scheduled in any of the ten business days following the date of cancellation (or notification of the delay, as applicable), and You will fully reimburse AppDynamics for any travel and expenses incurred by AppDynamics for such Services (and for any Services rescheduled by You) for which AppDynamics is unable to obtain a refund. In the event that the Vendor may be eligible to be reimbursed for travel expenses arising under the performance of this Contract, reimbursement will be at the out-of-state rates set forth in GS §138-6; as amended from time to time.

c) Paragraph 2.C “Data Protection, Privacy, and Confidential Information” is reserved.

d) The following language is hereby added to the Offer Description: AppDynamics: Notwithstanding anything to the contrary in the Agreement:

1. You will own any and all data and information that You configure the Software to collect, which is supplied to AppDynamics in accordance with any agreements between the You and AppDynamics (excluding any AppDynamics intellectual property therein);
2. AppDynamics and its suppliers own and shall retain all intellectual property rights, in and to the Software and the results of any Services (except for any of Your pre-existing intellectual property rights).
3. AppDynamics grants to You, during the License Term, a non-exclusive, non-transferable, licence to use the results of any Services for the purposes of making full

use of the Software."

4. The warranty provided in the AppDynamics Offer Description shall take precedence over any other conflicting warranty within the Agreement.

7) Sales or purchases shall not be completed unless such are authorized, where authorized sales or purchases have received approval for completion by DIT IT security, or delegation of IT security review and approval by DIT. Upon notice of a purchase under this Agreement, DIT procurement review will include an Agency's planned purchase to ensure security review together with identification of public and non-public data. Sales or purchases comprise any offers or procurements conducted directly by Vendor or through one or more resellers or other agents. The foregoing shall apply to goods or services placed or performed in State data centers or other Agency premises.

Except as modified herein, the AGREEMENT continues in effect as written and agreed.

Executed by authorized officials as of the day and date indicated below.

State of North Carolina
Department of Information Technology

DocuSigned by:
99B3638360B94A4...
Signature

Thomas Parrish
Printed Name of Signatory

9/29/2020 | 11:05 PM EDT
Date

Cisco Systems, Inc.

Signature

Jenn Pate

Authorized Signatory
Printed Name of Signatory

September 28, 2020
Date

APPROVED BY LEGAL

EXHIBIT A
AMENDMENT TWO
STATE TERM CONTRACT 204X
(IFB ITS-400277)

1. Cisco agrees to provide a Cyber Insurance Policy for the Cisco Cloud and SaaS product offerings provided under this Agreement. Cisco's Cyber Insurance Policy shall include, but is not limited to, the following:

    a. Coverage for unauthorized access to and unauthorized use of computer systems
    b. Coverage for regulatory proceedings alleging violation of privacy laws, whether common law or statutory law
    c. Coverage for business interruption and extra expense caused by a cyber event

2. The State approves the following Cisco Cloud/SaaS product offerings for use with non-public and public data. The State may modify this list as Cisco Cloud/SaaS products receive their FedRAMP Authority to Operate ("ATO") (or equivalent certification as determined by the State).
    - Cisco Cloudlock for Government
    - Unified Communications Manager Cloud for Government (Cisco UCM Cloud for Government)
    - Cisco WebEx Meetings
    - Duo Access
    - Web AppDynamic GovAPM

3. The State approves other Cisco Cloud/SaaS products within the scope of the contract (except as listed under Exhibit A, Paragraph 2) for use with public data only.