Illinois Department of Innovation and Technology Master Service Agreement

This Master Service Agreement ("**Agreement**") is made effective as of the date of last signature below ("**Effective date**") by and between the Illinois Department of Innovation and Technology, an Illinois State Agency with an address of 120 West Jefferson Street, Springfield, IL 62704 ("**DoIT**") and _____, a _____, with an address of _____ ("**Customer**"). Each may be referred to herein as a "**Party**" and collectively as the "**Parties**."

This Agreement terminates and supersedes any prior master service agreements entered into between Customer and DoIT.

PURPOSE

DoIT owns and operates a broadband backbone network ("**Illinois Century Network**" or "**ICN**" or "**DoIT Backbone Network**") with facilities for providing Intranet, Internet, security, and other services throughout the State of Illinois for its customers and constituents. DoIT also purchases Internet services and broadband circuits on behalf of and for its customers and constituents. DoIT issues individual master service agreements to provide these services to such customers and constituents.

ARTICLE 1 – GENERAL

1.1 Agreement Structure. The purpose of this Agreement is to provide general terms, conditions and a framework within which Customer may from time to time purchase certain transport, dedicated internet access and security services ("**Services**") from DoIT for its use. This Agreement and Service Orders (as defined in Section 1.2 below) and any other attachments incorporated therein shall collectively be referred to as the "**Agreement**."

1.2 Orders for Services. Working directly with the Customer, DoIT staff will help identify available connectivity and service options and will assist Customer throughout the provisioning, installation and turn-up of the Service. DoIT will prepare for the Customer a "**Service Order**," which will clearly identify the Service, monthly recurring charge ("**MRC**"), non-recurring charge ("**NRC**"), and Customer billing contact information and address. Once DoIT has received a signed copy of the Service Order from the Customer, DoIT will begin the provisioning of the Service. Each Service Order shall incorporate by reference, and shall be subject to, the terms and conditions of this Agreement, and the Service Level Agreement ("SLA") available at www.illinois.net when applicable. All Service Orders shall be subject to the availability of the Service requested and acceptance by DoIT. Customer acknowledges and agrees that Customer is solely responsible for the accuracy of all Service Orders and other information that it provides to DoIT.

1.3 Order of Precedence. In the event of an express conflict between a term(s) of this Agreement and the term(s) of any Service Order, precedence will be given in the following order: (a) the Service Order but solely with respect to the Service covered by that Service Order and provided that an authorized representative of DoIT has executed such Service Order; and (b) this Agreement.

1.4 Acceptable Use Policy. Customer agrees to be bound by DoIT's Acceptable Use Policy which may be found at www.illinois.net.

1.5 Cisco Products and Services. To the extent that Cisco Systems, Inc. ("**Cisco**") products and services are made available for Customer's use in connection with the Services provided under this MSA, Customer agrees to be bound by the terms and conditions of Appendix A (including Exhibit 1 and Exhibit 2) attached hereto and incorporated herein. DoIT shall have no liability to Customer for any claims or damages related to the Cisco products and services.

ARTICLE 2 – TERM

2.1 Agreement Term. This Agreement shall be in effect for a period of five (5) years from the Effective Date ("**Initial Term**") unless terminated earlier as otherwise provided for in this Agreement, and shall automatically renew for one (1) year periods thereafter (each a "**Renewal Term**") (Renewal Term(s) together with the Initial Term shall be referred to as the "**Term**") until either Party notifies the other Party of its intent not to renew the Agreement at least sixty (60) days prior to the end of the Initial Term or any Renewal Term. Notwithstanding the foregoing, in the event that a Service Order has a term longer than the Initial Term or Renewal Term of the Agreement stated herein, such Service Order remains in effect and this Agreement shall survive and govern and continue in effect with regard to only such Service Order until the termination of the Service Order.

2.2 Service Term. Each Service Order shall specify a period of time during which Customer may receive the applicable Services at the rates stated in the Service Order ("**Service Term**"). DoIT may commence work toward the provision of Services upon the Service Order Acceptance Date (as defined below), which may fall before the technical start date of the Service Term but which may still result in certain costs to Customer. Activation of Services will begin upon the Service Activation Date (as defined below) and will continue until the end of the Service Term specified in the Service Order, unless terminated earlier as otherwise provided for in this Agreement. Thereafter, unless otherwise stated in the Service Order, the Service Term of each such Service Order shall automatically renew for one (1) month periods (each a "**Service Renewal Term**") pursuant to the terms of the Agreement until terminated by either Party upon thirty (30) days written notice prior to the end of the Service Term or the then current Service Renewal Term; provided, however, that Customer shall continue to be responsible for payment to DoIT for the Services to be terminated through the end of the thirty (30) day notice period plus any early termination charges which may apply. Customer will not receive notice of a Service Term or Service Renewal Term expiration date. After the Service Term and during any Service Renewal Term, DoIT reserves the right to increase rates for any Services provided thereunder upon at least thirty (30) days' notice.

ARTICLE 3 – SERVICE ORDER PROCEDURE

3.1 To order a Service, Customer must execute a Service Order provided by DoIT. Customer may order additional Services from time to time by executing additional Service Orders. Upon receipt of a Service Order executed by Customer, DoIT will either: (a) accept the Service Order by way of counter-execution ("**Service Order Acceptance**"); (b) request clarification of information on the Service Order; or (c) reject the Service Order. DoIT shall be under no obligation to accept a Service Order. The date of DoIT's acceptance and counter-execution of the Service Order shall constitute the "**Service Order Acceptance Date**."

3.2 Following the Parties' mutual execution of a Service Order, DoIT will commence preparation work related to the Service Order and will notify Customer once a Service has been installed and activated ("**Service Activation Notice**"). The date of such notice shall constitute the "**Service Activation Date**;" provided, however, that if the Service is not initially accepted by Customer due to reasonable concerns that the Service does not conform with DoIT's specifications, DoIT shall address the alleged issues of non-conformance and issue a new Service Activation Notice, and the date of that new notice shall constitute the Service Activation Date. The Service shall be deemed accepted by Customer if (i) within seventy-two (72) hours following receipt of the Service Activation Notice, Customer does not notify DoIT in writing that the Services do not conform to DoIT's specifications (with evidence of such non-conformance included in the notice); (ii) DoIT has not performed the testing ensuring compliance with service specifications listed in the Service Order ("**Acceptance Testing**") due to Customer's failure to satisfy any of its obligations under this Agreement related to installation or activation; or (iii) Customer begins using the Service for any purpose other than testing.

ARTICLE 4 – BILLING AND PAYMENT

4.1 **Credit and Deposit**. If requested by DoIT, Customer shall complete and submit DoIT's standard credit application. DoIT may from time to time conduct a review of Customer's credit rating and payment history. DoIT may require Customer to pay a deposit before acceptance of a Service Order. Additionally, for any existing Services, DoIT may require (i) Customer to pay a deposit or (ii) an increase in the existing deposit, upon the failure of Customer to submit payment of any amount by the Due Date as a condition to the continued provision of such existing Services. DoIT shall refund any amount of deposit paid pursuant to this Section, less any amount for payments that Customer still owes to DoIT, when DoIT determines in good faith, based on Customer's credit rating and payment history, that such deposit is no longer necessary to ensure payment, but in no event later than after the termination of all Services and termination of this Agreement.

4.2 **Invoicing and Payment Terms**. DoIT will provide Customer with a monthly itemized invoice for the Services together with all other charges due. Customer shall pay DoIT all charges within 30 days of the invoice date or in accordance with the Illinois Local Government Prompt Payment Act (50 ILCS 505). Unless otherwise stated in the Service Order, DoIT may begin invoicing Customer for any NRC, or for any cancellation fees if applicable, upon the Service Order Acceptance Date. DoIT may invoice, and Customer shall be liable for, the applicable MRC payments for Services, or any early termination fees if applicable, beginning upon the Service Activation Date.

4.3 Invoice Disputes. To the extent that Customer disputes any portion of an invoice, Customer shall notify DoIT in writing and provide detailed documentation supporting its dispute within forty-five (45) days of the invoice date or the Customer's right to any billing adjustment shall be waived. In the event of a billing dispute, Customer shall timely pay all undisputed amounts. If the dispute is resolved against Customer, Customer shall pay such amounts due from the date the payment was originally due. A dispute may not be based upon a claim that all or a portion of the charges for the Services were incurred by unauthorized users. If the dispute is resolved against DoIT, DoIT will issue credit for the disputed amount outstanding or provide service credits for any payments made.

ARTICLE 5 – CANCELLATION

5.1 Cancellation. Customer may cancel a Service Order at any time prior to the Service Order Acceptance Date for such Service without any further liability. In the event Customer requests cancellation of a Service on or after the Service Order Acceptance Date and prior to the Service Activation Date for such Service, Customer shall be obligated to pay DoIT for any costs DoIT has incurred in provisioning the Service, including, but not limited to, any contracts entered into by DoIT in connection with this Agreement and any completed or incomplete installation services rendered, and the full cost of DoIT fiber and DoIT fiber facilities between the DoIT network and Customer property. If Customer requests cancellation at any time on or after the Service Activation Date, then Customer shall be liable for the early termination charges set forth in Article 6 below.

ARTICLE 6 – TERMINATION

6.1 Early Termination. In the event that Customer terminates any Service on or after the Service Activation Date but prior to the end of the Service Term or Service Renewal Term, or if DoIT terminates Services pursuant to a Customer Default, Customer shall be subject to early termination charges equal to (i) one hundred percent (100%) of all MRC for Services multiplied by the number of months remaining in the Service Term, or any Service Renewal Term, as the case may be; plus (ii) any and all installation charges, reasonable construction costs, charges from termination of third party services, or other charges or costs which have been incurred by DoIT in providing Customer with Services. Customer may exercise such right to terminate for convenience by providing at least thirty (30) days prior written notice. The Parties agree that the charges in this Section are a genuine estimate of DoIT's actual damages in the event Customer terminates for convenience and are not a penalty.

6.2 Termination for Cause. DoIT shall notify Customer of any breaches of the terms of this Agreement or of any Service Order by Customer, or any individual acting directly or indirectly under color of authority of Customer. Customer shall have thirty (30) days to cure such breach. In the event such breach is not cured within the thirty (30) days this Agreement may be terminated by DoIT without further notice, obligation or liability to Customer.

ARTICLE 7 – EQUIPMENT AND INSTALLATION

7.1 Customer Equipment. Customer, if requested by DoIT, shall provide a router or other connectivity equipment approved by DoIT for direct connection to the Network and to replace, at its expense, this equipment if it reaches the end of its useful life or at the expiration of the manufacture's support period. DoIT shall identify and install the equipment needed by Customer at its site to access the ICN if desired by the Customer. Customer is responsible for purchasing its own equipment. Unless Customer agrees to release DoIT of management responsibilities, DoIT shall monitor and support Customer's router or approved access device, for sites directly

connected to the ICN, in accordance with industry standards, provided Customer maintains at its sole expense a valid maintenance plan with equipment manufacturer. If, on responding to a Customer initiated service call, DoIT and Customer jointly determine that the cause of the service deficiency was a failure, malfunction or the inadequacy of equipment other than DoIT's Equipment or DoIT's Network, DoIT reserves the right to assess a fee for actual time and materials expended during the service call.

7.2 DoIT Access to Customer Premises. Where applicable, Customer shall provide DoIT with access to all Customer locations for purposes of installation, maintenance, and repair of DoIT Equipment on Customer premises. DoIT shall provide reasonable notice under the circumstance to Customer prior to entering Customer's point of presence to install, maintain or repair any of the DoIT Equipment. Customer will provide a safe place to work and comply with all applicable laws regarding the working conditions on the Customer premises.

7.3 DoIT Equipment. DoIT, or its agent, may provide, install, maintain, repair, operate and control DoIT's equipment including but not limited to fiber, conduit, man holes, hand holes, ducts, electrical and optical equipment ("**DoIT Equipment**"). DoIT Equipment shall remain the sole and exclusive property of DoIT, and nothing contained herein shall give or convey to Customer, or any other person, any right, title or interest whatsoever in DoIT Equipment, notwithstanding that it may be, or become, attached to, or embedded in, realty. Customer shall not tamper with, remove or conceal any identifying plates, tags or labels identifying DoIT's ownership interest in DoIT Equipment. Customer shall not adjust, align, attempt to repair, relocate or remove DoIT Equipment, except as expressly authorized in writing by DoIT. Customer shall be liable for any loss of or damage to DoIT Equipment caused by Customer's negligence, intentional acts, or unauthorized maintenance and shall reimburse DoIT for the same, within thirty (30) days after receipt by Customer of a request for reimbursement.

ARTICLE 8 – MAINTENANCE

8.1 Maintenance. DoIT shall maintain a 24x7x365 Network Operations Center (NOC) which will monitor the network and respond to customer calls and emails, perform network troubleshooting and engage network engineers and teams to resolve network issues, work with network and Internet Service Providers to resolve problems, and utilize a trouble ticketing program to track all incidences. NOC contact information is available at the Illinois Century Network website at www.illinois.net and may be reached by calling 312.814.3648 Option 2 or by email at doit.icn.noc@illinois.gov. DoIT shall perform regular and emergency maintenance on the network including upgrades to hardware and software, configuration changes or enhancements, or to increase network capacity and performance. DoIT has established maintenance windows as detailed at http://www.illinois.net. DoIT will perform emergency network maintenance outside of the maintenance window based on the urgency, as determined by DoIT, of the maintenance. Customers of the network will be notified by email at least five business days in advance of planned maintenance and DoIT will attempt, when reasonably possible, to notify customers by email for emergency maintenance outside the maintenance window.

ARTICLE 9 – DEFAULT; SUSPENSION OF SERVICE

9.1 Customer Default.

9.1.1 Customer is in default of this Agreement if Customer (a) fails to cure any monetary breach within five (5) days of receiving notice of the breach from DoIT; (b) fails to cure any non-monetary breach

of any terms of the agreement within thirty (30) days of receiving notice of the breach from DoIT; or (c) files or initiates proceedings or has proceedings filed or initiated against it, seeking liquidation, reorganization or other relief (such as the appointment of a trustee, receiver, liquidator, custodian or such other official) under any bankruptcy, insolvency or other similar law (each such event shall be a "**Customer Default**").

9.1.2 In the event of a Customer Default, DoIT may suspend Services to Customer until Customer remedies the Customer Default, or DoIT may terminate this Agreement and/or any or all of the Services being provided hereunder. DoIT may at its sole option, but without any obligation, cure a non-monetary breach at Customer's expense at any point and invoice Customer for the same. These remedies are in addition to and not a substitute for all other remedies contained in this Agreement or available to DoIT at law or in equity.

9.2 DoIT Default.

9.2.1 DoIT is in default of this Agreement if DoIT fails to cure any non-monetary breach of any material term of this Agreement within thirty (30) days of receiving written notice of the breach from Customer ("**DoIT Default**"); provided, however, that Customer expressly acknowledges that failure to meet the Service Availability Objectives in the SLA is not subject to a claim of a DoIT Default. Customer's exclusive remedies for any failure of DoIT to meet the Service Availability Objectives are set forth in the SLA.

9.2.2 In the event of a DoIT Default, Customer may terminate the Services and the Agreement upon written notice to DoIT. Any termination shall not relieve Customer of its obligations to pay all charges incurred hereunder prior to such termination.

ARTICLE 10 – IMPOSITIONS

10.1 All charges for the Services are exclusive of any Impositions (as defined below). Except for taxes based on DoIT's net income, Customer shall be responsible for payment of all applicable taxes that arise in any jurisdiction, including, without limitation, value added, consumption, sales, use, gross receipts, excise, access, bypass, franchise fees, rights of way fees or charges, license or permit fees, or other taxes, duties, fees, charges or surcharges (including regulatory fees), however designated, imposed on incident to, or based upon the provision, sale, or use of the Services ("**Impositions**"). Such Impositions may be shown on invoices as cost recovery fees. If Customer is entitled to an exemption from any Impositions, Customer is responsible for presenting DoIT with a valid exemption certificate (in a form reasonably acceptable to DoIT). DoIT will give effect to any valid exemption certificate provided in accordance with the foregoing sentence to the extent it applies to any Service billed by DoIT to Customer following DoIT's receipt of such exemption certificate. Customer shall indemnify, defend and hold DoIT harmless from payment and reporting of all such Impositions, including costs, expenses, and penalties incurred by DoIT in settling, defending or appealing any claims or actions brought against DoIT related to, or arising from, the non-payment of Impositions.

ARTICLE 11 – CONFIDENTIALITY

11.1 **Confidentiality**. Each Party, including its agents and subcontractors, to this Agreement may have or gain access to confidential data or information owned or maintained by the other Party in the course of carrying out its responsibilities under this Agreement. Customer shall presume all information received from DoIT or to which it gains access pursuant to this Agreement is confidential. Customer information, unless clearly marked as confidential and exempt from disclosure under the Illinois Freedom of Information Act, shall be considered public. No confidential data collected, maintained, or used in the course of performance of the Agreement shall be disseminated except as authorized or required by law either during the period of the contract or thereafter. The Customer must return any and all data collected, maintained, created or used in the course of the performance of the Agreement, in whatever form it is maintained, promptly at the end of the Agreement, or earlier at the request of DoIT, or notify DoIT in writing of its destruction. Any agent or subcontractor of Customer shall also be held to these confidentiality provisions, and Customer shall be responsible for any breach thereto by its agents or subcontractors. The foregoing obligations shall not apply to confidential data or information lawfully in the receiving Party's possession prior to its acquisition from the disclosing Party; received in good faith from a third-party not subject to any confidentiality obligation to the disclosing Party; now is or later becomes publicly known through no breach of confidentiality obligation by the receiving Party; or is independently developed by the receiving Party without the use or benefit of the disclosing Party's confidential information. Notwithstanding the above, nothing herein is intended to prevent or restrict DoIT or the State of Illinois from complying with all requirements of the Illinois Freedom of Information Act (5 ILCS 140).

ARTICLE 12 – CUSTOMER'S REPRESENTATIONS

12.1 Customer represents each of the following:

- It has all necessary power and authority to enter this Agreement and to perform all of its obligations hereunder and to manage and control and ensure each individual or entity that Customer authorizes, permits or allows to access the ICN or related services and equipment or facilities also complies with the terms of this Agreement in exercising such individual's access.
- This Agreement has been duly and validly authorized, executed and delivered by Customer and constitutes its valid and binding obligation.
- In performing its obligations hereunder, Customer will comply with all laws, rules and regulations of all governmental bodies having jurisdiction. Customer acknowledges that it is solely responsible for being aware of, and in compliance with, these applicable laws, rules and regulations, and that DoIT and the State of Illinois shall not be liable or responsible for Customer's failure to comply.
- Customer holds all required regulatory authorizations and permits to perform this Agreement according to its terms.
- Customer's obligations under this Agreement do not conflict with any other agreement.

ARTICLE 13 – DOIT'S REPRESENTATIONS

13.1 DoIT represents the following:

- DoIT has all necessary power and authority to enter this Agreement and to perform all of its obligations hereunder.
- This Agreement has been duly and validly authorized, executed and delivered by DoIT and constitutes its valid and binding obligation.
- In performing its obligations hereunder, DoIT will comply with all laws, rules and regulations of all governmental bodies having jurisdiction.
- DoIT holds all required regulatory authorizations and permits to provide the Services identified herein.

ARTICLE 14 – DISCLAIMER OF WARRANTY

14.1 DoIT and the State of Illinois disclaim all express or implied warranties, including without limitation, warranties of title, non-infringement, merchantability, or fitness for a particular purpose. Except as expressly set forth in the Agreement, customer assumes total responsibility for use of the Services.

In addition to any other disclaimers of warranty stated in the Agreement, DoIT and the State of Illinois make no warranty, guarantee, or representation, express or implied, that all security threats and vulnerabilities will be detected or that the performance of the Services will render Customer's systems invulnerable to security breaches, and DoIT shall not be responsible for any such vulnerability. Customer is responsible for Customer's own network security policy (including applicable firewall and Network Address Translation (NAT) policies) and security response procedures.

ARTICLE 15 – LIMITATION OF LIABILITY

15.1 Neither Party, the State of Illinois, their affiliates, agents, or contractors shall be liable for any indirect, incidental, special, reliance, punitive, or consequential damages or for any loss of, or cost to recover, data, use, business, revenues, profits, or goodwill relating to the services performed under this Agreement, or any action or omission relating to third parties, regardless of the legal theory under which such liability is asserted. Customer's indemnity obligations stated in this Agreement are exclusive of, and in no way limited by, this Section 15.1.

Any Customer claims relating to this Agreement must be brought within sixty (60) days following the end of the term or termination of the Services Order at issue.

ARTICLE 16 – LIMITATION OF SERVICE

16.1 Notwithstanding any other provision in this Agreement, this Agreement applies only to Services provided directly to the Customer for the Customer's use. These provisions shall not apply to offerings by the Customer for services to third parties. This Agreement does not constitute a joint undertaking for the furnishing of any service to customers or other third parties of the Customer. Services provided to the Customer under this Agreement may be connected to other facilities between certain locations and thereby constitute a portion of end-to-end service

furnished by the Customer to its customers or third parties. DoIT does not undertake to offer any services to any person or entity other than the Customer.

ARTICLE 17 – INDEMNIFICATION

17.1 To the extent allowed by law and subject to the terms and conditions set forth below, Customer agrees to indemnify, defend and hold harmless DoIT, its affiliates, the State of Illinois and their respective officers, officials, directors, employees and agents, from and against any and all liabilities, damages, taxes, tax penalties, claims, deficiencies, assessments, losses, suits, proceedings, actions, investigations, penalties, interest, costs and expenses of any kind, including without limitation, fees and expenses of counsel (whether suit is instituted or not and, if instituted, whether at trial or appellate levels) (collectively, the "Liabilities"), arising from or in connection with any and all claims, liens, damages, obligations, actions, suits, judgments, settlements or causes of action of every kind, nature and character, in connection with or arising out of the acts or omissions of Customer or its employees, representatives, contractors, agents, officers or officials, third parties of the Customer using the services provided in this Agreement, including any breaches or violations by Customer of any of the covenants or agreements contained in this Agreement. This Section shall not relieve Customer from any liability it may have for its own negligence or misconduct, whether by act or omission, and the negligence or misconduct, whether by act or omission, of its employees, agents, officers, officials and directors, representatives, or contractors. The obligations and covenants contained in this Section shall survive the expiration or termination of this Agreement.

ARTICLE 18 – FORCE MAJEURE

18.1 Notwithstanding anything to the contrary contained in this Agreement neither Party shall be liable for loss or damage or deemed to be in breach of this Agreement due to such Party's failure or delay of performance, wholly or in part, under this Agreement if such failure or delay of performance is due to causes beyond such Party's reasonable control ("Force Majeure Event"), including but not limited to: acts of God, fire, flood, explosion, storm or other catastrophic event; strikes or work stoppages; lockouts; acts of any government authority or of any civil or military authority including regulatory mandates; national emergencies, cable cut(s); sabotage; insurrections; riots; wars; and unforeseen acts of third Parties that cannot be avoided by acts of due care. Any delay resulting from a Force Majeure Event shall extend performance accordingly or excuse performance, in whole or in part, as may be reasonable.

ARTICLE 19 – MISCELLANEOUS PROVISIONS

19.1 IP Address Allocation Policy. DoIT shall provide all Internet Protocol ("**IP**") addresses needed for Customer and its equipment to use for the sole purpose of using the ICN to access the Internet and Intranet, provided that DoIT retains sole and absolute administrative control of each IP address provided, including without limitation, determining system requirements and deployment of each IP address, network scanning, monitoring system use, and denying assignment of or revoking assignments of addresses. Use of DoIT addresses on other provider networks without DoIT written consent is prohibited.

19.2 Network Security Management. DoIT staff routinely become aware of advanced persistent threats (APTs), or generally hostile state actors attacking state and local governments, universities and other ICN constituents. DoIT will provide network security and managed services, including scanning for vulnerabilities on

network systems, as further described in Appendix B, the terms and conditions of which are attached hereto and incorporated herein.

19.3 SLA Credits. All credits for any type of disruption in services shall be governed by the SLA. These credits shall be the Customer's sole and exclusive remedy for any disruption or interruption of the Services in this Agreement. The Customer must be in good standing with DoIT and the State of Illinois with respect to account receivables being current in order to submit a claim for, or receive, any credits.

19.4 Resale. For Services purchased or received under this Agreement, Customer shall prohibit, prevent, and not engage in any resale.

19.5 Connecting to ICN. For Services purchased or received under this Agreement Customer shall prohibit and prevent any other non-Customer entity from accessing, connecting to or interconnecting with the ICN in any manner or by any means.

19.6 Disruption of Service. DoIT reserves the right to block and/or terminate any connection to the ICN which is identified as causing a disruption of service on the backbone or to other customer connections and networks.

19.7 Applicable Law. This Agreement will be governed by the laws of the State of Illinois, without reference to its choice of law rules. Any claim against the State arising out of this Agreement must be filed exclusively with the Illinois Court of Claims (705 ILCS 505/1). The State shall not enter into binding arbitration to resolve any agreement dispute. The State of Illinois does not waive sovereign immunity by entering into this Agreement. The official text of cited statutes is incorporated by reference (An unofficial version can be viewed at www.ilga.gov/legislation/ilcs/ilcs.asp. In compliance with the Illinois and federal Constitutions, the Illinois Human Rights Act, the U. S. Civil Rights Act, and Section 504 of the federal Rehabilitation Act and other applicable laws and rules the State does not unlawfully discriminate in employment, contracts, or any other activity.

19.8 Right and Authority. Each of the Parties hereto represents and warrants to the other that this Agreement shall be binding upon and inure to the benefit of each of the Parties hereto and their respective agents, servants, employees, representatives, affiliates, heirs, executors, transferees, successors, and assigns, as the case may be.

19.9 Notices. If to DoIT: All inquiries and notices shall be, in writing, addressed to DoIT at 120 West Jefferson Street, Springfield, Illinois 62702, or by email at DoIT.ICN@illinois.gov.

If to Customer: All inquiries and notices shall be addressed to Customer using the contact information and addresses provided below, or by email at an email address designated by Customer.

For Administrative Notices:

For Billing Notices:

For Legal Notices:

For Maintenance Notices:

19.10 Use of Marks. Neither DoIT nor Customer shall directly or indirectly hold itself out as or otherwise create the impression that it is sponsored, authorized, endorsed by, affiliated with, or an agent of the other Party or affiliate or successor thereof, including but not limited to using the name DoIT or DoIT Backbone Network or ICN or the name of Customer, or of any affiliate, or any colorable imitation thereof in, or as part of, any DoIT or DoIT Backbone Network or ICN name or trade name (collectively, the "Marks"), or in any other confusing or misleading manner without the written consent of the other Party. The Parties acknowledge that all Marks are the exclusive property of the Party that is lawfully registered to hold such Marks. Customer may not utilize DoIT and DoIT Backbone Network and ICN Marks in its advertising without DoIT's prior written consent, and only as long as it complies with all policies and procedures pertaining to this use prescribed by DoIT from time to time. Customer shall not use the Marks for any other purpose without the express prior written consent of DoIT.

19.11 Severability. If any provision of this Agreement is declared or found to be illegal, unenforceable, or void, the Parties shall negotiate in good faith to agree on a substitute provision that is legal and enforceable and is as near as possible consistent with the intentions underlying the original provision. If the remainder of this Agreement is not materially affected by such declaration or finding and is capable of substantial performance, then the remainder shall be enforced to the extent permitted by law.

19.12 Interpretation. The construction of this Agreement shall not be construed against the Party causing its preparation but shall be interpreted on the basis of the plain meaning of the terms used which have been reviewed by both Parties in consultation with their respective counsel. Any provision of this Agreement officially declared void, unenforceable, or against public policy, shall be ignored and the remaining provisions shall be interpreted, as far as possible, to give effect to the Parties' intent. All provisions that by their nature would be expected to survive, shall survive termination. In the event of a conflict between DoIT's and Customer's terms, conditions and attachments, DoIT's terms, conditions and attachments shall prevail.

19.13 Availability of Appropriations (30 ILCS 500/20-60). This Agreement is contingent upon and subject to the availability of funds. DoIT, at its sole option, may terminate or suspend this Agreement, in whole or in part, without penalty or further payment or obligation being required, if (1) the Illinois General Assembly or the federal funding source fails to make an appropriation sufficient to pay or fulfill such obligation, or if funds needed are insufficient for any reason, (2) DoIT reserves funds, or the Governor decreases DoIT's funding by reserving some or all of DoIT's appropriation(s) pursuant to power delegated to the Governor by the Illinois General Assembly; or (3) DoIT determines, in its sole discretion or as directed by the Office of the Governor, that a reduction is necessary or advisable based upon actual or projected budgetary considerations. Customer will be notified in writing of the failure of appropriation or of a reduction or decrease.

19.14 Modifications. DoIT reserves the right to modify this Agreement at any time. DoIT shall provide 30 days prior written notice to Customer of any modification adopted by DoIT.

19.15 Assignability. Customer may not assign this Agreement or any of its obligations hereunder without DoIT's prior written consent.

19.16 Remedies. The rights and remedies of DoIT hereunder shall not be mutually exclusive; i.e., the exercise of one (1) or more of the provisions hereof shall not preclude the exercise of any other provision hereof. Customer

acknowledges, confirms and agrees that damages may be inadequate for a breach or a threatened breach of this Agreement and, in the event of a breach or threatened breach of any provision hereof, the respective rights and obligations hereunder shall be enforceable by specific performance, injunction or other equitable remedy. Nothing contained in this Agreement shall limit or affect any rights at law or by statute or otherwise for a breach or threatened breach of any provision hereof, it being the intent of this provision to clarify that the respective rights and obligations of the Parties shall be enforceable in equity as well as at law or otherwise.

19.17 FOIA. This Agreement and all related public records maintained by, provided to, or required to be provided to DoIT or the State of Illinois are subject to the Illinois Freedom of Information Act notwithstanding any provision to the contrary that may be found in this Agreement. 5 ILCS 140.

19.18 Entire Agreement. This Agreement, the Service Level Agreement, and all applicable Service Orders consists of all the terms and conditions contained herein which articulate the full and complete understanding of the Parties pertaining to the subject matter of this Agreement. This Agreement supersedes any prior or subsequent understandings, proposals, representations, discussions, and/or agreements (oral or written), absent a specific reference therein superseding this Agreement.

19.19 Headings. The section headings in this Agreement are inserted as a matter of convenience and in no way define, limit, or describe the scope of extent of such section, or affect the interpretation of this Agreement

19.20 No Third Party Rights. This agreement is made only between the Parties hereof and shall not establish rights in any third party as a third party beneficiary or otherwise.

19.21 Counterparts/Facsimile Signatures. This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. This Agreement may be delivered by facsimile transmission and facsimile signatures shall be treated as original signatures for all applicable purposes.

Department of Innovation and Technology (DoIT)		**[Customer name]**	
Signature:	_____	Signature:	_____
By:	_____	Printed Name:	_____
Printed Name:	_____	Date:	_____
Date:	_____	Title:	_____
Title:	_____		

NOTE: ***Pursuant to Section 1.5 of the Master Service Agreement ("MSA"), to the extent that Cisco Systems, Inc. ("Cisco") products and services are made available for Customer's use in connection with the Services provided under the MSA, Customer agrees to be bound by the terms and conditions of this Appendix A (including Exhibit 1 and Exhibit 2) attached hereto and incorporated herein. DoIT shall have no liability to Customer for any claims or damages related to the Cisco products and services.***

Appendix A

Cisco End User License Agreement

1. Scope and Applicability

1.1 This End User License Agreement ("**EULA**") between You and Cisco covers Your use of the Cisco Umbrella Software and Cloud Services ("**Cisco Technology**") distributed to You by Your Approved Source as part of their delivery of services to You in Your use of the Illinois Century Network. This document also incorporates any Product Specific Terms that may apply to the Cisco Technology, the Product Specific Terms set forth in Exhibits 1 and 2 for Appendix A. Definitions of capitalized terms are in Section 14 (Definitions).

1.2 You agree to be bound by the terms of this EULA through Your express agreement to this EULA.

2. Using Cisco Technology

2.1 **License and Right to Use**. Cisco grants You and Your Authorized Third Parties a non-exclusive, non-transferable (except as contemplated herein and under Your Approved Source's Enterprise Agreement Program Terms with Cisco):

(a) license to use the Software; and

(b) right to use the Cloud Services

both as acquired from Your Approved Source, for Your direct benefit during the Usage Term and as set out in Your Entitlement and this EULA (collectively, the "**Usage Rights**"). For the avoidance of doubt, You and Your Approved Source may freely change, at any time, which individuals/entities are associated or assigned to each license in the overall license count that is specified in Your Entitlement, within the required limit.

2.2 **Use by Third Parties**. You may permit Authorized Third Parties to exercise the Usage Rights on Your behalf, provided that such Authorized Third Parties comply with this EULA.

2.3 **Beta and Trial Use**. If Cisco grants You Usage Rights in the applicable Cisco Technology on a trial, evaluation, beta or other free-of-charge basis ("**Evaluation Software and Services**"):

(a) You may only use the Evaluation Software and Services on a temporary basis for the period limited by the license key or specified by Cisco in writing. If there is no period identified, such use is limited to 30 days after the Evaluation Software and Services are made available to You, unless otherwise agreed to by Cisco;

(b) If You fail to stop using and/or return the Evaluation Software and Services or the equipment on which it is authorized for use by the end of the trial period, You may be invoiced for use, however any invoicing will be subject to a new procurement or mutually agreed upon change order with the Approved Source as well as prior approvals from You and Your Approved Source and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9);

(c) Cisco, in its discretion, may stop providing the Evaluation Software and Services at any time, at which point You will no longer have access to any related data, information, and files through the Evaluation Software and Services and must cease using the Cisco Technology; in such event, to the extent practicably feasible and reasonable, Cisco will provide You the opportunity to receive a copy of any related data, information, and files in a non-proprietary format for Your own records; and

(d) The Evaluation Software and Services may not have been subject to Cisco's usual testing and quality assurance processes and may contain bugs, errors, or other issues. Except where agreed in writing by Cisco, You will not put Evaluation Software and Services into production use. Cisco provides Evaluation Software and Services "AS-IS" without support or any express or implied warranty or indemnity for any problems or issues. Cisco's will not have any liability relating to Your use of the Evaluation Software and Services.

2.4 **Upgrades or Additional Copies of Software.** You may only use Upgrades or additional copies of the Software beyond Your license Entitlement if You have:

(a) acquired such rights under a support agreement covering the applicable Software; or

(b) You have purchased the right to use Upgrades or additional copies separately, in which case such purchase will be subject to a new procurement or mutually agreed upon change order as well as prior approvals from You and Your Approved Source and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9) .

2.5 **Interoperability of Software.** If required by law and upon Your or Your Approved Source's request, Cisco will provide You with the information needed to achieve interoperability between the Software and another independently created program, provided You or Your Approved Source agree(s) to any additional terms reasonably determined by You or Your Approved Source and required by Cisco, and subject to Your or Your Approved Source's prior review and agreement. To the extent that such information constitutes Confidential Information as outlined in Section 5 below, You will hold it in confidence as permitted by applicable laws, regulations, and rules.

2.6 **No Subscription Renewal.** Usage Rights in Cisco Technology acquired on a subscription basis will not automatically renew.

3. Additional Conditions of Use

3.1 **Cisco Technology Generally.** Except as permitted herein and in Your Approved Source's Enterprise Agreement Program Terms with Cisco, and except as otherwise expressly agreed in writing by Cisco, You may not:

(a) transfer, sell, sublicense, monetize or make the functionality of any Cisco Technology available to any third party;

(b) use the Software on second hand or refurbished Cisco equipment not authorized by Cisco, or use Software that is licensed for a specific device on a different device (except as permitted by Cisco under Cisco's License Portability Policy located at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/policy/Software_License_Portability_Policy_FINAL.pdf or otherwise; for the avoidance of doubt, Cisco's License Portability Policy is not intended to impose any legal obligations on You; to the extent that Cisco's License Portability Policy has language that purports to impose any legal obligations on You, such language is not binding on or applicable to You);

(c) remove, modify, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks;

(d) reverse engineer, decompile, decrypt, disassemble, modify, or make derivative works of the Cisco Technology; or

(e) use Cisco Content other than as part of Your permitted use of the Cisco Technology.

3.2 **Cloud Services.** You will not intentionally:

(a) interfere with other customers' access to, or use of, the Cloud Service, or with its security;

(b) facilitate the attack or disruption of the Cloud Service, including a denial of service attack, unauthorized access, penetration testing, crawling or distribution of malware (including viruses, trojan horses, worms, time bombs, spyware, adware and cancelbots);

(c) cause an unusual spike or increase in Your use of the Cloud Service that negatively impacts the Cloud Service's operation; or

(d) submit any information that is not contemplated in the applicable Documentation.

3.3 **Evolving Cisco Technology**

(a) **Changes to Cloud Services.** Cisco may:

(1) enhance or refine a Cloud Service, although in doing so, Cisco will not materially reduce the core functionality of that Cloud Service, except as contemplated in this Section and 3.3(b); in such event, Cisco will notify You of the changes; and

(2) perform scheduled maintenance of the infrastructure and software used to provide a Cloud Service, during which time You may experience some reasonable temporary disruption to that Cloud Service. Where reasonably practicable, Cisco will provide You with reasonable advance written notice of such maintenance. You acknowledge that from time to time, Cisco

may need to perform emergency maintenance without providing You advance notice, during which time Cisco may temporarily suspend Your access to, and use of, the Cloud Service however Cisco shall use reasonable efforts to notify You as soon as possible of such emergency maintenance.

(b) **End of Life**

(1) Cisco may end the life of Cisco Technology, including component functionality ("**EOL**"), by providing prior written notice to You via Cisco's website at https://www.cisco.com/c/en/us/products/eos-eol-listing.html. Additionally, You may register for email notifications at https://www.cisco.com/c/en/us/support/web/tools/cns/notifications.html. For the avoidance of doubt, the information contained at the preceding weblinks is not intended to impose any legal obligations on You; to the extent that any content in the preceding weblinks contains language that purports to impose any legal obligations on You, such language is not binding on or applicable to You. If You or Your Approved Source prepaid a fee for Your use of Cisco Technology that becomes EOL before the expiration of Your then-current Usage Term, Cisco will use commercially reasonable efforts to transition You to a substantially similar Cisco Technology. If Cisco does not have substantially similar Cisco Technology, then Your Approved Source will receive a refund from Cisco or a Cisco Partner of any unused portion of the prepaid fee for the Cisco Technology that has been declared EOL ("**EOL Refund**").

(2) The EOL Refund will be calculated from the last date the applicable Cisco Technology is available to the last date of the applicable Usage Term.

3.4 **Protecting Account Access.** You will endeavor to keep all account information reasonably up to date, use reasonable means to protect Your account information, passwords and other login credentials, and promptly notify Cisco and Your Approved Source of any known or suspected unauthorized use of or access to Your account.

3.5 **Use with Third Party Products.** If You use the Cisco Technology together with third party products, such use is at Your risk. You are responsible for complying with any applicable third-party provider terms, provided that You shall have prior notice of the applicable terms and an opportunity to review and agree to such terms. Cisco does not provide support or guarantee ongoing integration support for third-party products that are not a native part or component of the Cisco Technology.

3.6 **Open Source Software.** Open source software not owned by Cisco is subject to separate license terms as set out at www.cisco.com/go/opensource. To the extent that any Cisco Technology contains open source software, the applicable open source software licenses will not materially or adversely affect Your ability to exercise Usage Rights in the applicable Cisco Technology.

4. Fees

If applicable, any fees for Your use of Cisco Technology are set out in Your agreed-upon purchase terms with Your Approved Source. If You use Cisco Technology beyond Your Entitlement ("**Overage**"), Your Approved Source may invoice You for such Overage; however, any invoicing is subject to a new procurement or mutually agreed upon change order as well as prior approvals from You and Your Approved Source and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9), and to the extent legally permitted, You agree to use reasonable efforts to obtain necessary approvals. If You cannot obtain necessary approvals, You will cease all use of the Overages.

5. Confidential Information and Use of Data

5.1 **Confidentiality**

(a) Recipient will hold in confidence and use no less than reasonable care to avoid disclosure of any Confidential Information (except that which is required to be disclosed pursuant to law enforcement, court order, or applicable laws, rules, and regulations, including the Illinois Freedom of Information Act (5 ILCS 140)) to any third party, except for its employees, affiliates and contractors who have a need to know ("**Permitted Recipients**").

Recipient must ensure that its Permitted Recipients are subject to confidentiality obligations no less restrictive than the Recipient's obligations under this EULA.

(b) Such nondisclosure obligations will not apply to information:

(1) which is known by Recipient without confidentiality obligations;

(2) which is or has become public knowledge through no fault of Recipient;

(3) which is independently developed by Recipient; or

(4) to the extent it is required to be disclosed pursuant to law enforcement, court order, or applicable laws, rules, and regulations, including but not limited to the Illinois Freedom of Information Act (30 ILCS 500).

(c) Recipient may disclose Discloser's Confidential Information if required under a regulation, law or court order. Recipient will reasonably cooperate, subject to prior approval and discretion of the Illinois Attorney General (if You are Recipient), at Discloser's expense, regarding protective actions pursued by Discloser.

(d) Upon the reasonable request of Discloser, Recipient will either return, delete or destroy all Confidential Information of Discloser, except that You may retain Cisco's Confidential Information to the extent that it is required to be retained by applicable laws, rules, or regulations.

5.2 **How We Use Data.** Cisco will access, process and use data in connection with Your use of the Cisco Technology in accordance with applicable privacy and data protection laws. For further details, visit Cisco's Security and Trust Center at https://www.cisco.com/c/en/us/about/trust-center/systems-information.html. For the avoidance of doubt, the information contained at https://www.cisco.com/c/en/us/about/trust-center/systems-information.html is not intended to impose any additional obligations on You. To the extent that https://www.cisco.com/c/en/us/about/trust-center/systems-information.html contains content with language that purports to impose obligations on You, such language is not binding on or applicable to You.

5.3 **Notice and Consent.** To the extent Your use of the Cisco Technology requires it in compliance with applicable law, You are responsible for providing notice to and obtaining consents from individuals, to the extent legally necessary, regarding the collection, processing, transfer and storage of their data through Your use of the Cisco Technology.

6. Ownership

6.1 Except where agreed in writing and as is otherwise provided in this EULA and Your Approved Source's Enterprise Agreement Program Terms with Cisco, nothing in this EULA transfers ownership in, or grants any other license to, any intellectual property rights. You retain any ownership of Your content and Cisco retains ownership of the Cisco Technology and Cisco Content. To the extent that use of the Cisco Technology results in any of Your (or the Authorized Third Parties' or Your Approved Source's) Customer Content being collected, used, stored, or maintained by Cisco, Cisco must (i) return such content and data in a non-proprietary format, at Your request; or (ii) notify You in writing of its destruction. "Customer Content" means data, such as text, audio, video or image files, provided by You (or the Authorized Third Parties or Your Approved Source) to Cisco in the use of the Cisco Technology.

6.2 Cisco may use feedback You provide in connection with Your use of the Cisco Technology as part of its general business operations and for providing You the Cisco Technology contemplated herein.

7. Indemnification

7.1 **Claims.** Cisco will defend any third party claim against You that Your valid use of Cisco Technology under Your Entitlement infringes a third party's patent, copyright, trade secret, registered trademark, or any other intellectual property right (the "**IP Claim**"). Cisco will hold You harmless and indemnify You against the final judgment entered by a court of competent jurisdiction or any settlements arising out of an IP Claim. You shall:

(a) promptly notify Cisco and Your Approved Source in writing of the IP Claim;

(b) reasonably cooperate with Cisco (and Your Approved Source to the extent applicable) in the defense of the IP Claim, subject to the prior approval and discretion of the Illinois Attorney General; and

(c) Subject to the prior approval and discretion of the Illinois Attorney General, grant Cisco the right to exclusively control the defense and settlement of the IP Claim, and any subsequent appeal.

7.2 **Additional Remedies.** If an IP Claim is made and prevents Your exercise of the Usage Rights, Cisco will either procure for You the right to continue using the Cisco Technology, for which cost will be borne exclusively by Cisco, or replace or modify the Cisco Technology with functionality that is at least equivalent. If Cisco or Your Approved Source determine(s) that these alternatives are not reasonably available or functional for Your use, either party may terminate Your Usage Rights granted under this EULA upon written notice to the all parties, and Cisco or the Cisco Partner will refund Your Approved Source a prorated portion of the fee Your Approved Source paid for the Cisco Technology for the remainder of the unexpired Usage Term.

7.3 **Exclusions.** Cisco has no obligation with respect to any IP Claim that would not have occurred but for:

(a) Cisco's compliance with any designs, specifications, or requirements provided by You, or by a third party specifically designated and authorized by You in writing to provide such information;

(b) Your unauthorized modification of any Cisco Technology, or the unauthorized modification by a third party;

(c) unrelated services that you provide to users in connection with the Cisco Technology; for the avoidance of doubt, Cisco shall remain liable where an IP Claim arises from an authorized use of Cisco Technology;

(d) the unauthorized combination, operation, or use of the Cisco Technology with non-Cisco products, software or business processes;

(e) Your failure to modify or replace the Cisco Technology as reasonably required by Cisco, provided that You received at least ten (10) business days' prior written notice from Cisco that the modification or replacement was necessary to avoid potential infringement; or

(f) Any Cisco Technology provided on a no charge, beta, or evaluation basis.

This Section 7 states Cisco's entire obligation and Your exclusive remedy regarding any IP Claim against You.

8. Warranties and Representations

8.1 **Performance.** Cisco warrants that:

(a) for a period of 90 days from the Delivery Date or longer as stated in Documentation, or on www.cisco.com/go/warranty, the Software substantially complies with the Documentation (For the avoidance of doubt, the information contained at www.cisco.com/go/warranty is not intended to impose any additional obligations on You. To the extent that www.cisco.com/go/warranty contains content or language that purports to impose additional obligations on You, such language is not binding on or applicable to You); and

(b) during the Usage Term, it provides the Cloud Services with commercially reasonable skill and care in accordance with the Documentation and Product Specific Terms.

8.2 **Malicious Code.** Cisco warrants that it will use commercially reasonable efforts to deliver Cisco Technology free of Malicious Code, and will not intentionally introduce Malicious Code into the Cisco Technology.

8.3 **Qualifications.**

(a) Sections 8.1 and 8.2 do not apply if the Cisco Technology or the equipment on which it is authorized for use:

(1) has been altered, except by Cisco or its authorized representative; for clarity, alterations contemplated are not intended to apply to user-adjustable settings present in the Cisco Technology,

(2) has been subjected to abnormal physical conditions, accident, or negligence, or unauthorized installation or unauthorized use inconsistent with this EULA or Cisco's instructions;

(3) is acquired on a no charge, beta or evaluation basis;

(4) is not a Cisco-branded product or service; or

(5) has not been provided by an Approved Source.

(b) Upon Your prompt written notification to the Approved Source during the warranty period of Cisco's breach of this Section 8, Your and Your Approved Source's sole and exclusive remedy (unless otherwise required by applicable law) is, at Cisco's option, either:

(1) repair or replacement of the applicable Cisco Technology at Cisco's sole cost with functionality that is at least equivalent; or

(2) a refund of either:

(A) the license fees paid for the non-conforming Software; or

(B) the fees paid for the period in which the Cloud Service did not comply, excluding amounts paid by Cisco under an applicable service level agreement.

(c) Where Cisco provides a refund of license fees for Software, You must cease use of and return or destroy all copies of the applicable Software except as required to be retained by applicable laws, rules or regulations.

(d) **Except as expressly stated in this EULA, to the extent allowed by applicable law, Cisco expressly disclaims all other warranties and conditions of any kind, express or implied, including without limitation any warranty, condition or other implied term as to merchantability, fitness for a particular purpose or non-infringement, or that the Cisco Technology will be uninterrupted or error-free.**

(e) If You are a consumer, You may have legal rights in Your country of residence that prohibit the limitations set out in this Section from applying to You, and, to the extent where prohibited, they will not apply.

9. Liability

9.1 Neither party will be liable for indirect, incidental, exemplary, special, punitive, or consequential damages; or interruption or loss of business; or loss of revenues, profits, goodwill or anticipated sales or savings. Where any loss or corruption of data arising from the use of the Cisco Technology is due to Cisco's negligent or intentional acts and omissions (i) in the performance of services onsite at Your or an Authorized Third Party's location, Cisco will reimburse You (or Your Approved Source if applicable) for the actual and reasonable costs of restoring the data, or (ii) where Cisco is obligated to store Your or an Authorized Third Party's data, Cisco will be responsible for restoring the data, with both (i) and (ii) being subject to the liability limitation in Section 9.2 below.

9.2 Except for Cisco's indemnification obligations and bodily injury damages to person (including death) and property, Cisco's maximum aggregate liability under this EULA, in conjunction with all claims arising from all entities receiving the Cisco Technology under this EULA from Your Approved Source, is limited to: (a) for claims arising from Software licensed on a perpetual basis, the fees paid or payable by Your Approved Source for that Software or (b) for all other claims arising from Cisco Technology, the fees paid or payable by Your Approved Source for the applicable Cisco Technology for the subscription term period of the Cisco Technology that first gave rise to the liability.

9.3 This limitation of liability applies whether the claims are in warranty, contract, tort (including negligence), or otherwise, even if either party has been advised of the possibility of such damages. Nothing in this EULA limits or excludes any liability that cannot be limited or excluded under applicable law. This limitation of liability is cumulative and not per incident.

10. Termination and Suspension

10.1 **Termination**

(a) If a party materially breaches this EULA and does not cure that breach within 30 days after receipt of written notice of the breach, the non-breaching party may terminate this EULA for cause. During the cure period and upon written notification to You and Your Approved Source, Cisco may suspend Your Usage Rights if You have materially breached sections 3.1 (Cisco Technology), 3.2 (Cloud Services) or 13.7 (Export). For the avoidance of doubt, issues related to delayed payment shall not be considered a material breach.

(b) Upon termination of the EULA, You must stop using the Cisco Technology and destroy any copies of Software and Confidential Information within Your control, unless required by law to be retained.

(c) If this EULA is terminated due to Cisco's material breach, Cisco will refund Your Approved Source, the prorated portion of fees Your Approved Source has prepaid for the Usage Rights beyond the date of termination.

11. Verification

11.1 During the Usage Term and for a period of 12 months after its expiration or termination, You will take reasonable steps to maintain complete and accurate records of Your use of the Cisco Technology sufficient to verify compliance with this EULA ("**Verification Records**"). Upon reasonable advance notice, and no more than once per 12 month period, You will, within 30 days from Cisco's written notice, allow Cisco and its auditors reasonable access to the Verification Records and any applicable books, systems (including Cisco product(s) or other equipment), and accounts at a time agreed to by You in advance and during Your normal business hours.

11.2 If the verification process discloses underpayment of fees:

(a) Any payment of fees not authorized under the applicable Entitlement shall be subject to a new procurement or mutually agreed upon change order as well as prior approvals from You and Your Approved Source and the requirements and limitations of applicable laws, rules, and regulations,

including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

12. Security and Data Protection Requirements

12.1 Cisco and its affiliates, representatives, agents, employees, and subcontractors shall only access Your and Your Approved Source's and the Authorized Third Parties' Customer Content, networks, and systems when such access is necessary to provide or otherwise deliver Cisco Technology and services contemplated herein.

12.2 Cisco shall implement appropriate administrative, physical, and technical safeguards to protect Customer Content that are consistent with accepted industry practices. Cisco shall ensure that all such safeguards, including the manner in which information or data is collected, accessed, used, stored, processed, disposed of, and disclosed, comply with data protection and privacy laws applicable to Cisco in performing its obligations under this EULA. Cisco shall not access or attain any personally identifiable information, protected classes of information, or other sensitive information while providing the services contemplated herein, except as contemplated in the applicable offer description and data privacy sheets and in compliance with applicable laws, rules, and regulations, and Cisco agrees that any such information shall be protected in the same manner as is Confidential Information.

12.3 Cisco shall have a documented security incident policy and plan and must provide a copy at Your Approved Source's reasonable request.

12.4 Where Cisco has undertaken independent third-party audit Statement on Standards for Attestation Engagements ("**SSAE-18**") certifications for particular Cisco Technology, upon request by Your Approved Source, Cisco will provide annual copies of its applicable System Operation Controls 2 ("**SOC2**") report(s) and/or bridge/gap letter(s).

12.5 Cisco will notify the State of Illinois Chief Information Security Officer at DoIT.ICN@illinois.gov within forty-eight (48) hours, or sooner as required by applicable, laws, rules, and regulations, of confirmation of any information breach or other security incident that impacts State of Illinois Customer Content. Cisco will use diligent efforts to remedy any such breach or incident in a timely manner to prevent a reoccurrence. Cisco will reimburse You (or Your Approved Source, if applicable) the costs of mitigating damages and of providing legally required notifications to affected individuals.

13. General Provisions

13.1 **Survival**. Sections 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14 survive termination or expiration of this EULA.

13.2 **Third Party Beneficiaries**. This EULA does not grant any right or cause of action to any third party.

13.3 **Assignment and Subcontracting.**

Neither party may assign or novate this EULA in whole or in part without the other party's express written consent.

13.4 **U. S. Government End Users.** The Software, Cloud Services and Documentation are deemed to be "commercial computer software" and "commercial computer software documentation" pursuant to FAR 12.212 and DFARS 227.7202. All U.S. Government end users acquire the Software, Cloud Services and Documentation with only those rights set forth in this EULA. Any provisions that are inconsistent with federal procurement regulations are not enforceable against the U.S. Government. As You are not an entity of the U.S. Government, the foregoing is not applicable to Your use of the Cisco Technology

13.5 **Modifications to the EULA**. Any modifications to this EULA must be agreed to in writing by Your Approved Source (or You, if permitted by Your Approved Source) and Cisco.

13.6 **Compliance with Laws**

(a) **General.** Each party will comply with all laws and regulations applicable to their respective obligations under this EULA. For the avoidance of doubt, all Cisco Affiliates performing services under this EULA and under Your Approved Source's Enterprise Agreement Program Terms with Cisco will comply with all applicable laws, rules and regulations including but not limited to the Illinois Procurement Code (30 ILCS 500), as such are applicable to Cisco and Affiliates. Cisco may restrict the availability of Cisco Technology in any particular location or modify or discontinue features to comply with applicable laws and regulations, provided that Cisco shall notify Your Approved Source of modifications or discontinuations that affect Your or Your Approved Source's use of the Cisco Technology. In the event that such modifications of discontinuations materially or adversely impact Your or Your Approved Source's use, Your Approved Source may terminate the order and will receive

a refund from Cisco or a Cisco Partner of any fees Your Approved Source has prepaid for the remaining unused portion of the applicable order.

13.7 **Export**. Cisco's Software, Cloud Services, products, technology and services (collectively the "**Cisco Products**") are subject to U.S. and local export control and sanctions laws. You acknowledge and agree to the applicability of and Your compliance with those laws, and You will not knowingly receive, use, transfer, export or re-export any Cisco Products in a way that would cause Cisco to violate those laws. You also agree to obtain any legally required licenses or authorizations for export.

13.8 **Governing Law and Venue.** This EULA, and any disputes arising from it, will be governed by the laws of the State of Illinois. The Parties hereby submit to the exclusive jurisdiction of the Illinois Court of Claims (705 ILCS 505), or, if applicable and permitted by law and the Illinois Attorney General, a U.S. District Court located in the State of Illinois, for any question or dispute arising out of or relating to this Agreement.

13.9 **Notice**. Any notice delivered by Cisco to You and Your Approved Source under this EULA will be delivered via email or regular mail or the postings at Cisco.com referenced herein. Notices to Cisco should be sent to Cisco Systems, Office of General Counsel, 170 Tasman Drive, San Jose, CA 95134 unless this EULA, applicable Product Specific Terms, or an order specifically allows other means of notice.

13.10 **Force Majeure.** Neither party will be responsible for failure to perform its obligations due to an unforeseeable event or circumstances beyond its reasonable control and not due to its negligence. Your Approved Source may terminate this agreement without penalty or further obligation if performance does not resume within thirty (30) days of Cisco's written notice to Your Approved Source that it intends to exercise this provision.

13.11 **No Waiver.** Failure by either party to enforce any right under this EULA will not waive that right.

13.12 **Severability.** If any portion of this EULA is not enforceable, it will not affect any other terms.

13.13 **Entire agreement.** This EULA is the complete agreement between the parties with respect to the subject matter of this EULA and supersedes all prior or contemporaneous communications, understandings or agreements (whether written or oral).

13.14 **Translations**. Cisco may provide local language translations of this EULA in some locations. You agree that those translations are provided for informational purposes only and if there is any inconsistency, the English version of this EULA will prevail.

13.15 **Order of Precedence**. If there is any conflict between this EULA and any Product Specific Terms expressly referenced in this EULA (set forth in Exhibits 1 and 2), the order of precedence is:

(a) Such Product Specific Terms;

(b) this EULA (excluding the Product Specific Terms and any Cisco policies); then

(c) any applicable Cisco policy expressly referenced in this EULA.

14. Definitions

"**Affiliate**" means any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where "control" means to: (a) own more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means.

"**Approved Source**" as it relates to the State of Illinois's Entitlement means Cisco or a Cisco Partner; and Approved Sources as it relates to Your Entitlement means the State of Illinois providing Cisco Technology through the Illinois Century Network.

"**Authorized Third Parties**" means Your Users, Affiliates, third party service providers, and each of their respective Users, permitted to access and use the Cisco Technology on Your behalf as part of Your Entitlement.

"**Cisco**" "**we**" "**our**" or "**us**" means Cisco Systems, Inc. or its applicable Affiliate(s).

"**Cisco Content**" means any:

(a) content or data provided by Cisco to You as part of Your use of the Cisco Technology; and

(b) content or data that the Cisco Technology generates or derives in connection with Your use.

Cisco Content includes geographic and domain information, rules, signatures, threat intelligence and data feeds and Cisco's compilation of suspicious URLs.

"**Cisco Partner**" means a Cisco authorized reseller, distributor or systems integrator authorized by Cisco to sell Cisco Technology.

"**Cloud Service**" means the Cisco hosted software-as-a-service offering or other Cisco cloud-enabled feature described in the applicable Product Specific Terms. Cloud Service includes applicable Documentation and may also include Software.

"**Confidential Information**" means non-public proprietary information of the disclosing party ("**Discloser**") obtained by the receiving party ("**Recipient**") in connection with this EULA, which:

(a) is conspicuously marked as confidential or if verbally disclosed, is immediately at the time of disclosure noted to be confidential and is promptly summarized thereafter in writing to Recipient and marked confidential within three days of verbal disclosure; and

(b) is exempt from disclosure under the Illinois Freedom of Information Act (5 ILCS 140).

"**Delivery Date**" means the date agreed in Your Approved Source's Entitlement, or where no date is set forth, the date that Cisco makes the Cisco Technology available to Your Approved Source for use or download and installation, provided that services shall not be deemed to have started or been delivered prior to the date Your Approved Source has executed an order with the Cisco Partner.

"**Documentation**" means the technical specifications and usage materials officially published by Cisco specifying the functionalities and capabilities of the applicable Cisco Technology. For the avoidance of doubt, the information contained in the relevant Documentation is not intended to impose any additional obligations on You. To the extent that the applicable Documentation contains content or language that purports to impose additional obligations on You, such language is not binding on or applicable to You.

"**Entitlement**" means the specific metrics, duration, and quantity of Cisco Technology that You acquire from Your Approved Source through Your mutually executed agreement with Your Approved Source.

"**Malicious Code**" means code that is designed or intended to disable or impede the normal operation of, or provide unauthorized access to, networks, systems, Software or Cloud Services other than as intended by the Cisco Technology (for example, as part of some of Cisco's security products); which may include but is not limited to, viruses, worms, trap doors, back doors, timers, clocks, counters, or other limiting routines, instructions, or designs that would erase data or programming or that would otherwise cause the products or services to become inoperable or incapable of being used in the manner for which they were designed or in accordance with any Documentation.

"**Product Specific Terms**" means additional product-related terms, including offer descriptions, applicable to the Cisco Technology You acquire as set forth in Exhibits 1 and 2 to Appendix A.

"**Software**" means the Cisco computer programs, including Upgrades, firmware and applicable Documentation.

"**Upgrades**" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software.

"**Usage Term**" means the period commencing on the Delivery Date and continuing until expiration or termination of the Entitlement, during which period You have the right to use the applicable Cisco Technology.

"**User**" means the individuals (including, contractors, or employees) permitted to access and use the Cisco Technology on Your behalf as part of Your Entitlement. User also includes K-12 educators, staff, and student users who You allow to use the Cisco Technology contemplated in this EULA as part of receiving services from Your Approved Source.

"**You,**" "Your," "End User," or "Customer" means the entity receiving the Cisco Technology from the State of Illinois through the Illinois Century Network.

cisco SECURE

Exhibit 1 to Appendix A
Offer Description: Cisco Umbrella

This Offer Description (the **"Offer Description"**) describes Cisco Umbrella (the "Cloud Service"). Your subscription is governed by this Offer Description and the Cisco End User License set forth in Appendix A (the **"Agreement"**). Capitalized terms used in this Offer Description and not otherwise defined herein have the meaning given to them in the Agreement.

1. Description

Cisco Umbrella is a cloud security platform that unifies multiple security services in a single cloud-delivered platform to secure internet access and control cloud app usage from your network, branch offices, and roaming users. Depending on the package and deployment, Cisco Umbrella integrates secure web gateway, cloud-delivered firewall ("CDFW"), domain name service ("DNS") -layer security, cloud malware protection and cloud access security broker ("CASB") functionality for effective protection anywhere users go. Before users connect to any online destination, Cisco Umbrella acts as a secure onramp to the internet and delivers deep inspection and control to support compliance and block threats. Cisco Umbrella is backed by one of the largest threat intelligence teams in the world, Cisco Talos, and it provides interactive access to threat intelligence through Cisco Umbrella Investigate to aid in incident response and threat research. Cisco Umbrella Investigate provides access to certain Cisco threat intelligence about malicious domains, internet protocols addresses ("IPs"), networks, and file hashes. Using a diverse dataset of billions of daily DNS requests and live views of the connections between different networks on the internet, Cisco applies statistical models and human intelligence to identify attackers' infrastructures. Cisco Umbrella Investigate data can be accessed via a web-based console or an application programming interface ("API"). Please consult the Umbrella Documentation for further information on its technical specifications, configuration requirements, features and functionalities. For the avoidance of doubt, the information contained in the Umbrella Documentation is not intended to impose any additional obligations on You or Your Approved Source. To the extent that the Umbrella Documentation contains content or language that purports to impose additional obligations on You or Your Approved Source, such language is not binding on or applicable to You or Your Approved Source.

Your Cisco Umbrella subscription includes access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence (through SecureX threat response, also known as Cisco Threat Response), unifies visibility across various Cisco and third party security products, enables automated workflows, and more. For more information on SecureX, please see the SecureX Offer Description set forth in Exhibit 2 to Appendix A.

Applicability of Offer Description Sections to Products included in Umbrella Suite

Package	Applicable Sections of this Offer Description
Umbrella for Education*	1, 2.1, 2.2, 2.8, 3, 4, 5
Umbrella Insights	1, 2.1, 2.2, 2.8, 3, 4, 5
Umbrella Platform	1, 2.1, 2.2, 2.8, 3, 4, 5
Umbrella DNS Advantage	1, 2.1, 2.2, 2.3 (if purchasing the CDFW add-on), 2.5 (if purchasing the CDFW add-on), 2.6, 2.8, 3, 4, 5
Umbrella SIG Essentials	1, 2.1, 2.2, 2.4, 2.5, 2.8, 3, 4, 5
Umbrella Investigate API*	1, 2.1, 2.2, 2.7 (if purchasing UMB-INV-CONSOLE-SP and/or UMB-INV-INT-API-SP) 2.8, 3, 4, 5

Your current subscription includes Umbrella for Education and Umbrella Investigate API. Products may be changed or added at the discretion of Your Approved Source, subject to prior State of Illinois approvals and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

2. Supplemental Terms and Conditions

2.1. Restrictions

If You are an authorized Cisco service provider whose contract with Cisco authorizes You to utilize Cisco cloud services on behalf of end customers, You may use the Cloud Service only for the benefit of such end customers.

2.2. Disclaimers

EXCEPT AS PROVIDED IN THE AGREEMENT, CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY

ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS.

2.3. Cisco Umbrella Cloud Delivered Firewall – DNS Security Add-On for Layers 3 and 4 ("CDFW L3/4")

CDFW L3/4 Bandwidth: CDFW L3/4 is licensed by megabits per second ("Mbps") and the total amount of Mbps that Your Approved Source is licensed to use is the "Subscribed Bandwidth." Cisco will continuously measure usage of CDFW L3/4 throughout a given month by analyzing the previous thirty (30) day period for peaks in Mbps on Your network. If at any time, Cisco determines that Your Approved Source's 95th Percentile Bandwidth (defined below) has exceeded the Subscribed Bandwidth, Cisco reserves the right to either throttle the bandwidth and/or work with Your Approved Source to determine an appropriate remedy in accordance with Your Approved Source's agreement with Cisco and/or the Cisco Partner as applicable, including by way of example, Your reduction in usage to the purchased quantity, or if that is not feasible, the purchase of additional license. To the extent Your Approved Source determines that Your Approved Source need to increase the Subscribed Bandwidth, any additional purchase shall be subject to a potential new procurement, prior State of Illinois approvals, and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

The 95th Percentile Bandwidth is calculated by observing Your Mbps peaks over the course of thirty (30) days, with the first thirty (30) day period beginning upon activation of the Cloud Service, and discarding the top 5% of the Mbps peaks observed in that time frame. The next highest Mbps peak value after discarding the top 5% Mbps peaks is Your "95th Percentile Bandwidth." For example, if there are one hundred (100) Mbps peaks observed, Cisco would discard the top five (5) Mbps peaks and the next highest Mbps peak is Your 95th Percentile Bandwidth. So, if the highest six (6) Mbps peaks were measured as 22Mbps, 25Mbps, 28Mbps, 35Mbps, 27Mbps, and 24Mpbs for that thirty (30) day period, Your 95th Percentile Bandwidth would be 22Mbps.

2.4. Cisco Umbrella Secure Internet Gateway Essentials ("SIG Essentials")

The following use limitations apply in connection with Your use of Cisco Umbrella Secure Internet Gateway Essentials and Cisco Umbrella Secure Internet Gateway SIG Essentials Add-On (collectively, "SIG Essentials").

SIG Essentials is licensed based on the quantity of Covered Users and is subject to an Average Bandwidth (as defined below) limit of 50 kilobits per second ("kbps"). "Covered Users" means the total number of internet-connected individuals authorized to use the applicable Software or Cloud Service under Your Approved Source's agreement with Cisco and/or the Cisco Partner, as applicable.
Cisco will continuously measure Your Approved Source's total usage of SIG Essentials throughout a rolling thirty (30) day period to determine the Average Bandwidth. If at any time Cisco determines that the Average Bandwidth has exceeded 50 kbps, then Your Approved must reduce the Average Bandwidth, or Cisco may work with Your Approved Source to determine an appropriate remedy in accordance with Your Approved Source's agreement with Cisco and/or the Cisco Partner, as applicable, including by way of example, a reduction in usage to the purchased quantity or if that is not feasible Your Approved Source's purchase of additional licenses. To the extent Your Approved Source determines that Your Approved Source needs to purchase additional licenses as required to reduce the Average Bandwidth to 50 kbps, any such additional purchase shall be subject to a potential new procurement, prior State of Illinois approvals, and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

The formula for Average Bandwidth is:

Average Bandwidth = 95th Percentile Bandwidth / Number of Covered Users

The 95th Percentile Bandwidth is calculated by: (i) observing total traffic samples under Your Approved Source over the course of thirty
(30) days at each Cisco Umbrella data center the traffic is sent to, (ii) discarding the top 5% of the traffic samples at each such data center and taking the next highest traffic sample value ("Peak Value"), and (iii) adding together the Peak Value for each data center. Traffic samples for purposes of this calculation

include DNS traffic, secure web gateway (proxy) traffic and CDFW traffic (Layer 3, Layer 4 and if applicable, Layer 7).

For example, if the Peak Value at one data center is 1,000,000 kbps and the Peak Value at a second data center Your traffic is sent to is 10,000 kbps, the 95th Percentile Bandwidth is 1,000,000 + 10,000 = 1,010,000 kbps. The Average Bandwidth would be 1,010,000 kbps divided by the number of Covered Users licensed under Your Approved Source's subscription. If Your Approved Source has 25,000 users covered by Your Approved Source's subscription, then the Average per user Bandwidth for the monitored period is 1,010,000 / 25,000 = 40.4 kbps.

2.5. Cloud Delivered Firewall and SIG Essentials

In connection with Your use of Cisco Umbrella Cloud Delivered Firewall and/or SIG Essentials, You will not knowingly (and will not knowingly allow any third party to): (i) use the Cloud Service to run automated queries to external websites; (ii) use the Cloud Service to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use the Cloud Service for the purpose of intentionally masking Your identity in connection with the commission of unlawful activities or to otherwise avoid legal process. Additionally, by using either of these Cloud Services, You acknowledge that in the event that Cisco receives a third party demand letter or other legal inquiry with regards to alleged unlawful activity on Your network, Cisco may disclose Your name to such third party solely as necessary to comply with legal processes, meet national security requirements, or as otherwise required by applicable law.

2.6. DNS Security Essentials and DNS Security Advantage ("DNS Security")

The following use limitations apply in connection with Your use of Cisco Umbrella DNS Security Essentials and DNS Security Advantage (collectively, "DNS Security").

DNS Security is licensed based on the quantity of Covered Users and is subject to a Monthly DNS Query Average (as defined below) limit of three thousand (3,000) DNS queries per User per day. Cisco will continuously monitor Your usage of DNS Security on a monthly basis to determine

Your Monthly DNS Query Average. If at any time Cisco determines that Monthly DNS Query Average under Your Approved Source has exceeded three thousand (3,000) DNS queries per Covered User per day, then Your Approved Source must reduce the Monthly DNS Query Average, or Cisco may work with Your Approved Source to determine an appropriate remedy in accordance with Your Approved Source's agreement with Cisco or Cisco Partner, as applicable, including by way of example, their reduction in usage to the purchased quantity or if that is not feasible Your Approved Source's purchase of additional licenses. To the extent Your Approved Source determine(s) that Your Approved Source needs to purchase additional licenses, any such additional purchase shall be subject to a potential new procurement, prior State of Illinois approvals, and the requirements and limitations of applicable laws, rules, and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

Monthly DNS Query Average = (number of DNS queries in applicable month / number of days in applicable month) / number of licensed Covered Users

For example, if Your Approved Source purchased licenses for 1,000 Covered Users and the Covered Users submitted a total of 3,000,000 DNS queries in the prior 30-day month, the Monthly DNS Query Average is asfollows:

(3,000,000 / 30) / 1,000 = 100

2.7. Cisco Umbrella Investigate for MSSP

Notwithstanding anything to the contrary in the Agreement, if Your Approved Source purchased a Cisco Umbrella Investigate for MSSP SKU labeled UMB-INV-CONSOLE-SP and/or UMB-INV-INT-API-SP (collectively, "Investigate for MSSP"), You may use Investigate for MSSP as a tool to perform research and generate reports for the benefit of Your third party customers solely as part of connectivity, management, and/or administrative services You provide to Your third party customers.

Any co-branding of Investigate for MSSP by You shall be subject to the guidelines located here: https://www.cisco.com/c/dam/en/us/products/collateral/security/umbrella/umbrella-sps-co-branding-guidelines.pdf and any additional intellectual property and trademark guidelines set forth in the

Agreement. For clarity, if You provide any research, data, or results generated from Your use of Investigate for MSSP to Your third party customers, You must at all times credit Cisco as the source of such information following the above guidelines.

2.8. Cisco-Managed S3 Log Storage

Certain Cisco Umbrella packages include the ability to select Cisco-managed S3 storage or company-managed storage (i.e. Your own storage) for DNS, proxy and event logs. Cisco-managed S3 log storage is available with 7, 14 or 30 day retention options. If You require more than 30 days retention, You should select company-managed storage or export the data from the Cisco-managed storage to Your company-managed storage prior to the expiration of the retention period.

3. Service Level Agreement

For purposes of this Service Availability Commitment, "Service" shall be defined as Cisco's recursive DNS service and does not include web-based user interfaces, configuration systems or other data access or manipulation methods. Cisco shall use commercially reasonable efforts to maintain Cisco Umbrella Service availability of 99.999% of each calendar month. Availability will be calculated by dividing the total number of minutes of Uptime (defined below) during the applicable calendar month by the total number of minutes in such month, minus minutes of Cisco Umbrella Service Outages (defined below) occurring due to scheduled maintenance and attributable to Third Party Actions (defined below), and multiplying that amount by 100. The formula for this calculation is as follows:

$$\text{Availability} = (X, Y) \times 100$$

X= Total # of minutes of Uptime during calendar month

Y= (Total # of minutes in such calendar month) - (Total # of minutes of Outages from scheduled maintenance and Third Party Actions)

For the purposes of this calculation, (i) an "Outage" means Cisco Umbrella is completely unreachable when Your Internet connection is working correctly, (ii) "Uptime" means the number of minutes where there were no Cisco Umbrella Service Outages, excluding Outages for scheduled maintenance and Third Party Actions, and (iii) "Third Party Action" means any action beyond Cisco's reasonable control and not caused by Cisco, including, without limitation, the performance of Internet networks controlled by other companies or traffic exchange points that are controlled by other companies, labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortages. If a dispute arises about whether or not an Outage occurred, Cisco and You shall work together to make a determination in good faith based on system logs, monitoring reports, and configuration records. Cisco shall not be responsible for any Cisco Umbrella Outages arising out of Third Party Actions.

4. Data Protection

Cisco's data protection obligations are set forth in the Agreement and in Your Approved Source's agreement with Cisco. The Cisco Umbrella, Cisco Threat Response, and Cisco SecureX Privacy Data Sheets (available at https://trustportal.cisco.com, and copies of which are attached hereto) describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services. Additionally, Cisco Umbrella Insights, Cisco Umbrella Platform, Cisco Umbrella Secure Internet Gateway (SIG) Essentials, Cisco Umbrella DNS Security Advantage, and Cisco Umbrella Secure Internet Gateway (SIG) Essentials Add-on package(s) leverage(s) the Cisco Advanced Malware Protection (AMP) Ecosystem. Please see the AMP Ecosystem Privacy Data Sheet (attached hereto and available at: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=AMP#/pdfViewer/c%2Fdam%2Fr%2Fctp%2Fdocs%2Fprivacydatasheet%2Fsecurity%2Fcisco-orbital-advanced-search-privacy-data-sheet.pdf). For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center located at https://www.cisco.com/c/en/us/about/trust-center/systems-information.html. For the avoidance of doubt, the information contained at https://www.cisco.com/c/en/us/about/trust-center/systems-information.html and in the Privacy Data Sheets (including any information in other weblinks associated with or contained within the Privacy Data Sheets) is not intended to impose any additional obligations on You or Your Approved Source. To the extent that https://www.cisco.com/c/en/us/about/trust-center/systems-information.html or the Privacy

Data Sheets (including any weblinks associated with or contained within the Privacy Data sheets) contain content that purports to impose obligations on You or Your Approved Source, such language is not binding on or applicable to You or Your Approved Source. The Privacy Data Sheet provides the process for You to request deletion of data.

5. Support & Maintenance

5.1. Technical Support

Cisco Umbrella services purchased under Your Approved Source's Security Choice Enterprise Agreement include online support and phone support at the Enhanced Level set forth below. Cisco will respond as set forth in the table below and may require information from You to resolve service issues. You agree to provide the information reasonably requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Phone Support provides Cisco Technical Assistance Center ("TAC") access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Enhanced	24x7 via Phone & Web	Response within 30 minutes	Response within 2 hours

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

Severity 1 means the service is unavailable or down or there is a critical impact to a significant impact to case submitter's business operation. Case submitter and Cisco will work in good faith to resolve the situation which may include committing full-time resources as applicable. For avoidance of doubt, the IT representative from each K-12 school may be a case submitter.

Severity 2 means the service is degraded or significant aspects of case submitter's business operation are negatively impacted by unacceptable software performance. Case submitter and Cisco will work in good faith to resolve the situation which may include committing full-time resources during Standard Business Hours as applicable.

Severity 3 means the service is impaired, although most business operations remain functional. Case submitter and Cisco will work in good faith to resolve the situation which may include committing full-time resources during Standard Business Hours as applicable.

Severity 4 means minor intermittent functionality or performance issue with the service, or information is required, as applicable. There is little or no impact to case submitter's business operation. Case submitter and Cisco both are willing to work in good faith to provide resources during Standard Business Hours to provide assistance or information as requested.

Business Day means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco and case submitter.

Standard Business Hours means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

cisco SECURE

Exhibit 2 to Appendix A
Offer Description: Cisco SecureX

This Offer Description (the **"Offer Description"**) describes Cisco SecureX, a cloud feature included with most Cisco security products (the **"Cloud Service" or "SecureX").** Your use of Cisco SecureX is governed by this Offer Description and the Cisco End User License Agreement between You and Cisco (the **"Agreement", set forth in Appendix A**). Capitalized terms used in this Offer Description and not otherwise defined herein have the meaning given to them in the Agreement.

1. Description

SecureX is a cloud-based feature available through many of Cisco's security products which consists of several functional elements. SecureX threat response, also known as Cisco Threat Response (CTR), acts as an aggregator of threat intelligence collected or generated by the applicable Cisco security products, as well as available third-party products selected by a customer. SecureX orchestration enables design and automation of workflows involving Cisco and third-party products. The SecureX dashboard makes it possible to visualize key security metrics and trends using data provided by platform products in a single location. SecureX ribbon provides users with access to important notifications, data, and product functionality while users navigate between supporting Cisco products.

2. Supplemental Terms and Conditions

2.1. Disclaimers

EXCEPT AS PROVIDED IN THE AGREEMENT, CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS. SECUREX ORCHESTRATION ENABLES CUSTOMERS TO PROGRAM AUTOMATED WORKFLOWS. CUSTOMERS ARE RESPONSIBLE FOR ENSURING THAT WORKFLOWS ARE PROGRAMMED CAREFULLY, IN ACCORDANCE WITH THE TECHNICAL DOCUMENTATION SUPPLIED BY CISCO AND WITH CONSIDERATION FOR HOW THAT WORKFLOW MIGHT OPERATE UNDER POTENTIAL DIFFERING CIRCUMSTANCES. CISCO RECOMMENDS ALL WORKFLOWS BE TESTED IN A NON-PRODUCTION ENVIRONMENT PRIOR TO IMPLEMENTATION IN PRODUCTION.

3. Data Protection

The Cisco SecureX, Cisco SecureX Sign-On, and Cisco SecureX threat response Privacy Data Sheet(s) describe the Personal Data that Cisco collects and processes as part of the delivery of SecureX. For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center located at https://www.cisco.com/c/en/us/about/trust-center/systems-information.html. For the avoidance of doubt, the information contained at https://www.cisco.com/c/en/us/about/trust-center/systems-information.html and in the Privacy Data Sheets (including any information in other weblinks associated with or contained within the Privacy Data Sheets) is not intended to impose any additional obligations on You or Your Approved Source. To the extent that https://www.cisco.com/c/en/us/about/trust-center/systems-information.html or the Privacy Data Sheets (including any weblinks associated with or contained within the Privacy Data sheets) contain content that purports to impose obligations on You or Your Approved Source, such language is not binding on or applicable to You or Your Approved Source.

4. Support & Maintenance

SecureX is a cloud-based feature available through most of Cisco's security products and support for SecureX is included with the applicable support service covering such products.

Appendix B

Network Security Management

DoIT is continually working to secure the ICN and protect the ICN from cybersecurity threats and vulnerabilities. These efforts include securing the interconnect points between the ICN and Customer, vulnerability scanning, and monitoring network traffic for potential security vulnerabilities and malicious activity ("**DoIT Security Services**"). A security threat to the ICN may result from a security attack on the Customer network (for example, an attack on an internet protocol ("**IP**") address used by a Customer). Thus, DoIT prevention and mitigation of security attacks may also prevent and mitigate certain security attacks on Customer's network.

DoIT operates a Security Operations Center ("**SOC**") that has capability to monitor network traffic for potential security vulnerabilities and malicious activity, and that can further provide security consulting and testing services.

Customer hereby acknowledges and agrees to the following provisions:

1.1 DoIT may provide Customer certain security services that include auto distributed denial of service protection, firewall, intrusion detection, vulnerability scanning ("**Customer Security Services**") to prevent and mitigate security attacks on Customer's network.

1.2 During the operation of DoIT Security Services or Customer Security Services, DoIT may have access to cyber activity data, including but not limited to source and destination IP addresses.

1.3 DoIT's Security Operations Center may monitor Customer's traffic for any malicious activity. "**Malicious activity**" may include any computer code, IP address, or website that can cause damage or a virus to a computer or system.

1.4 DoIT may conduct real-time monitoring and analysis of source and destination IP addresses and header information, as well as potential areas in Customer's external facing systems that are vulnerable to compromise or attack. In doing so, DoIT may identify and investigate potential cyber threats to Customer.

1.5 In the event that DoIT detects any vulnerabilities or malicious activity in Customer's data, DoIT may use best efforts to alert Customer as soon as reasonably practicable.

1.6 Customer agrees to cooperate with DoIT to prevent and mitigate security attacks on both the Customer network and on the ICN.

1.7 Customer Security Services or DoIT Security Services, including any alerts, information, findings, recommendations, reports, results, or conclusions, are provided on an "as is" basis with no warranties or representations of any kind. DoIT makes no warranty, express or implied, that all security threats and vulnerabilities will be detected or that the Customer Security Services or DoIT Security Services themselves will render Customer's network and systems safe from malicious code, intrusions, or other security breaches. Outside of provisions identified in the SLA (see Member Service Agreement, Article 1, Section 1.2), DoIT shall have no liability for damages or costs that may be caused by Customer Security Services or DoIT Security Services, for any intrusions by any third party, for any interruptions in service that may occur, or for any damage to Customer data or devices that may result, and DoIT shall not be responsible for failure to identify, prevent, remedy, or cure malicious activity that may cause damage to Customer's computers or systems.