Exhibit A

OSI

V2.1 Nov.16, 2020 City edits 12062021

Cyber Security Supply Chain Risk Management Agreement between Open Systems International, Inc. and the City of Columbia

This Cyber Security Supply Chain Risk Management Agreement ("Agreement") is entered by and between Open Systems International, Inc. (hereinafter "Contractor") and the City of Columbia (hereinafter "City"). The Agreement sets forth the terms and conditions relating to the Critical Infrastructure Protection ("CIP") reliability standard CIP-013-1: Cyber Security – Supply Chain Risk Management ("CIP-013") Requirement R1.2 relating to security controls for vendors. The terms contained in this Agreement are an addition to the terms of the Software Implementation Services Agreement, and any subsequent contracts between the Parties for additional services (collectively "Services Agreement"). The Agreement is a "Contract Document" as that term is used in the Services Agreement; nothing in this Agreement alters the terms in the Services Agreement. The Agreement is effective on the date of signing by the party last executing this Agreement ("Effective Date").

NOW, THEREFORE, the Parties hereto, for good and sufficient consideration, the receipt of which is hereby acknowledged, intending to be legally bound, do hereby agree as follows.

Definitions

The following definitions apply only to the terms and conditions in this Agreement:

"***CEII***" means Critical Energy Infrastructure Information and/or Critical Electric Infrastructure Information.

"***Contractor***" means the Open Systems International Inc. (OSI) in relation to supplying a product or service.

"***City***" means the City of Columbia Missouri, which is the organization that acquires or acquired or procures or procured a product or service.

"***City Information***" means for purposes of these terms and conditions, any and all information concerning City and its business in any form, including, without limitation, the products and services provided under this Agreement that is disclosed to or otherwise learned by Contractor during the performance of this Agreement. Such Information must be reduced in writing and clearly identified as confidential and/or proprietary.

"***Disclosed***" means any circumstance when the security, integrity, or confidentiality of any City Information has been compromised, including but not limited to incidents where City Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose.

"***PII***" means Personally Identifiable Information.

"***Restricted Information***" means any City information that is additionally and clearly identified by the City as Restricted Information under applicable statutes and/or regulations such as CEII or BES Cyber System Information (BCSI) information as defined by the Glossary and that is considered highly confidential where disclosure outside of the City may result in significant loss of intellectual property, personally identifiable information, may cause damage to the operational effectiveness or otherwise substantially disrupt significant business operations, with examples including but not limited to, source code, encryption private keys, or City CEII or bulk electric systems (BES) Cyber System Information (BCSI) information as defined by NERC.

"***Security Incident***" means when Contractor confirms that (1) Restricted Information in the possession of the Contractor has been Disclosed and such disclosure materially affects the City Restricted Information, or (2) an incident has occurred that materially and adversely affects products and services provided by Contractor.

1. Notification of Contractor-identified incidents (Requirement R1.2.1)

Contractor agrees to notify City within 72 hours by email at noc-nerc@como.gov whenever Contractor confirms that a Security Incident has occurred and materially impacts the City Information or products and/or services provided by Contractor.

To the extent that Contractor is the cause of a Security Incident and as legally possible, Contractor will send a communication to City stating the nature and extent of the incident, the data affected, the proposed remedial action, and the timeframe for remediation, to the best of its knowledge at the time the communication is provided. Contractor will then work with the City to the extent necessary and as mutually agreed by the parties, to implement any resolution of the incident. Additionally, and to the extent Contractor is the actual cause of any incident, Contractor will take all reasonable steps to support City's internal investigation of any such incident and reasonably respond to City requests for information regarding such incident, except to the extent such requests would require the disclosure of personal, confidential, or proprietary information.

2. Coordination of responses to Contractor – identified incidents (Requirement R1.2.2)

Development and Implementation of a Response Plan: Contractor shall maintain and regularly update policies and procedures to prevent and address Security Incidents ("Response Plan"), as determined in the reasonable judgement of Contractor, by mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence to prevent the recurrence of the same or similar Security Incidents in the future. The development and implementation of the Response Plan shall follow best practices that at a minimum are consistent with the contingency planning requirements of ISO-27002, Section 16 - "Information Security Incident Management" and/or more broadly, the NIST Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide."

In the event of a Security Incident related to the products and services provided to City, Contractor shall implement its Response Plan and, within 48 hours of implementing its Response Plan, shall notify City of that implementation by email at the address identified in paragraph 1.

Prevention of Recurrence: Within a commercially reasonable time after the occurrence of a Security Incident, Contractor agrees to take all reasonable steps that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and ISO-27002, Section 16 - "Information Security Incident Management" and Contractor may also provide recommendations to City on actions that City may take to assist in the prevention of recurrence, as applicable or appropriate.

Coordination of Incident Response with City: Within a commercially reasonable time of notifying City of the Security Incident, Contractor shall recommend actions to be taken by City on City-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Contractor shall coordinate with City in developing those action plans and mitigating controls. Contractor will take all reasonable steps to provide City guidance and recommendations, and other reasonably necessary information for recovery efforts and for long term remediation and/or mitigation of cyber security risks posed to City Information, equipment, systems, and networks as well as any information necessary to assist City in any recovery efforts undertaken by City in response to the Security Incident.

Notification to Affected Parties:

To the extent Contractor is the cause of a Security Incident, Contractor will, at its sole cost and expense, assist and cooperate with City with respect to any investigation of a Security Incident, disclosures to affected parties, and other remedial measures as requested by City in connection with a Security Incident or required under any applicable laws related to a Security Incident.

In the event a Security Incident results solely in City Information being Disclosed, not including other Contractor client's information, such that notification is required to be made to any person or entity, including without limitation any customer or current or former employee of City under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by City, with Contractor's consent to the contents of such notice, except as required by applicable law or approved by City in writing. City will have sole control over the timing and method of providing such notification. To the extent required by applicable law, For Security Incidents that affect multiple Contractor clients, Contractor will directly notify appropriate governmental authorities, and use all reasonable efforts to coordinate with City regarding any further notification.

3. Termination of Access Control of Contractor Representatives (Requirement R1.2.3)

Development and Implementation of Access Control Policy: Contractor shall maintain policies and procedures to address the security of remote and onsite access to City Information, City systems and networks, and City property (an "Access Control Policy") that is consistent with the personnel management requirements of ISO-27002, Section 9 "*Access Control*" and also meets the following requirements.

- City Authority Over Access: In the course of furnishing products and services to City , Contractor shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Contractor Personnel") to access City's property, systems, or networks or City Information without City's prior express written authorization. Such written authorization may subsequently be revoked by City at any time in its sole discretion. Further, any Contractor Personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by City. All City authorized connectivity or attempted connectivity to City's systems or networks shall be in conformity with City's security policies as may be amended from time to time with notice to the Contractor.

- Contractor Review of Access: Contractor will review and verify Contractor Personnel's continued need for access and level of access to City Information and City systems, networks and property on a semi-annual basis and will retain evidence of the reviews for two years from the date of each review.

- City Review of Access: City will review and verify City employee's need for access and level of access to Contractor Information and Contractor systems, networks and property on a quarterly basis and notify Contractor when City employee's access should be removed.

- Notification and Revocation: Contractor will notify City within 72 hours in writing at the email address identified in paragraph 1 (no later than 12 hours of termination per "(ii)" set forth below no later than 24 hours) and will immediately take all steps necessary to remove Contractor Personnel's access to any City Information, systems, networks, or property when:

  (i) any Contractor Personnel no longer requires such access in order to furnish the services or products provided by Contractor,
  (ii) any Contractor Personnel is terminated or suspended or his or her employment is otherwise ended,
  (iii) Contractor reasonably believes any Contractor Personnel poses a threat to the safe working environment at or to any City property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or employee or City Information,
  (iv) there are any material adverse changes to any Contractor Personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record,
  (v) any Contractor Personnel fails to maintain conduct in accordance with the qualification criteria set forth in Contractors documented adjudication criteria.
  (vi) any Contractor Personnel loses his or her U.S. work authorization, or
  (vii) Contractor's provision of products and services to City is either completed or terminated, so that City can discontinue electronic and/or physical access for such Contractor Personnel.

Contractor will take all steps reasonably necessary to immediately deny such Contractor Personnel electronic and physical access to City Information as well as City property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multi-factor security tokens, and laptops, as applicable, and will return to City any City-issued property including, but not limited to, City photo ID badge, keys, parking pass, documents, or laptop in the possession of such Contractor Personnel. Contractor will notify City at the email address identified in paragraph 1, once access to City Information as well as City property, systems, and networks has been removed.

4. Contractor Vulnerability Disclosure and Remediation (Requirement R1.2.4)

Contractor shall maintain policies and procedures to address the disclosure and remediation by Contractor of vulnerabilities and material defects related to the products and services provided to City, including the following:

(a) Prior to the delivery of the procured product or service, Contractor shall provide summary documentation of all publicly disclosed vulnerabilities and material defects in the procured Contractor product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

(b) Contractor shall follow a "Coordinated Vulnerability Disclosure" policy as documented in ISO-29147 "Vulnerability Disclosure", NIST Cybersecurity Framework version 1.1. RS-AN-5 and further detailed in the whitepaper "*CERT Guide to Coordinated Vulnerability Disclosure*" by Carnegie Mellon: https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf. The Contractor policy will ensure that vulnerabilities are not disclosed publicly until a mitigation is available. Possible mitigations include a software patch/update, configuration change, , procedural work-around, firewall policy change, etc. Vulnerabilities will be prioritized and mitigated according to their criticality in an Industrial Control System environment. Upon failing to provide a mitigation, Contractor shall when possible, publish a recommended method of exploit detection, without disclosing technical details that might enable exploitation of the vulnerability itself. The details of the Contractor policy are incorporated into its "*Vulnerability Management Policy*", made available upon request.

(c) Contractor shall disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written documentation that all such backdoors created by Contractor have been permanently remediated.

(d) Contractor shall implement a vulnerability detection and remediation program consistent with 5 RA-5,17 SA-11,18, or ISO-27002, Section 14.2 – Security in development and support processes requirements.

Disclosure of Vulnerabilities by City: Whether or not publicly disclosed by Contractor and notwithstanding any other limitation in this Agreement, City may disclose any Contractor vulnerabilities or material defects in the products and services provided by Contractor to (a) the Electricity Information Sharing and Analysis Center, the Industrial Control Systems Cyber Emergency Response Team, or any equivalent U.S. governmental entity, (b) to any U.S. governmental entity when necessary to preserve the reliability of the BES as determined by City in its reasonable judgement, or (c) any entity required by applicable law. For the avoidance of doubt, City may only disclose the minimum amount of information necessary to satisfy its legal obligation to any governing body. Further, this paragraph does not relieve, and still requires, that City complies with the Confidentiality provisions of any applicable contract terms of this agreement.

5. Verification of software integrity and authenticity (Requirement R1.2.5)

Hardware, Firmware, Software, and Patch Integrity and Authenticity:

(a) Contractor shall maintain risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided to City. Contractor shall provide documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on how to request replacement parts, to the extent possible commitment from its third party manufacturers to ensure that, for a period of at least one year, spare parts shall be made available by Contractor based upon availability of all sub-components.

(b) Contractor shall specify how digital delivery for procured products (*e.g.*, software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If City deems that it is warranted, Contractor shall apply encryption to protect procured digital products throughout the delivery process.

(c) If Contractor provides software or patches to City, Contractor shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable City to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from Contractor's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Contractor.

(d) Contractor shall identify or provide City with a method to identify the country (or countries) of origin of the procured Contractor product and its top level components (including hardware, software, and firmware) to the extent Contractor can reasonably obtain such information. Contractor will identify to the extent reasonably possible the countries where the development, manufacturing, maintenance, and service for the Contractor product are provided.

(e) Contractor shall provide a top level summary software bill of materials for procured (including licensed) Contractor products.

(f) Contractor shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

(g) Contractor shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

(h) Contractor shall maintain chain-of-custody documentation demonstrating internal handling for procured products and require tamper-evident packaging for the delivery of hardware to the City.

Patching Governance:

(a) Prior to the delivery of any products and services to City or any connection of electronic devices, assets or equipment to City's electronic equipment, Contractor shall follow ISO-27001 requirements regarding its patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for Contractor products, services, and any electronic device, asset, or equipment required by the Contractor to be connected to the assets of City during the provision of products and services . This documentation may, to the extent deemed applicable by Contractor, include information regarding: (i) the resources and technical capabilities to sustain this program and process such as the method or recommendation for how the integrity of a patch is validated by City; and (ii) the approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

(b) Unless otherwise approved by the City in writing, current or supported version of Contractor products and services shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components (*e.g.*, Java, Flash, Web browser, etc.).

(c) Contractor shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to City.

(d) In providing the products and services described in Services Agreement, Contractor shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered applicable vulnerabilities or weaknesses for Contractor products as identified within section 4-b) of this document within a commercially reasonable timeframe.

(e) When third-party hardware, software (including open-source software), and firmware is incorporated/embedded into products provided by Contractor to City, to the extent reasonably possible, Contractor shall provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses if applicable to the City's use of the third-party product in its system environment, within 60 days of its availability from the original supplier and/or patching source. To the extent Contractor is capable, updates to remediate critical vulnerabilities applicable to the Contractor's use of third part product in its system environment shall be prioritized and provided within a shorter period than other updates, within 30 days of its availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested, and made available by Contractor within these time periods, Contractor shall provide or arrange for the provision of recommended mitigations and/or workarounds to the extent possible within a commercially reasonable timeframe.

<u>Viruses, Firmware and Malware</u>:

(a) Contractor will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to City.

(b) As of the time of delivery, Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any Contractor software or patches, and Contractor will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality in violation of this agreement or any other licenses provided under an applicable agreement.

(c) When install files, scripts, firmware, or other Contractor delivered software solutions are flagged as malicious, infected, or suspicious by a Contractor supported anti-virus vendor Contractor will to the extent possible and commercially reasonable provide technical background as to why the software should be considered a "false positive" to ensure their code's supply chain has not been compromised.

(d) To the extent that, a virus or other malware is found to have been coded or otherwise introduced as a direct result of Contractor's negligence or recklessness under this Agreement, Contractor shall upon written request by City and at its own cost:

(i) Take all necessary remedial action and provide assistance to City to eliminate the virus or other malware throughout City's information networks, computer systems, and information systems, and

(ii) If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Contractor is obligated under this Agreement to back up such data, take all steps necessary and provide all assistance required by City and its affiliates, or (B) where Contractor is not obligated under this Agreement to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

<u>End of Life Operating Systems</u>:

(a) Contractor delivered solutions will not be required to reside on end-of-life operating systems, or any Contractor approved operating system that will go end-of-life six (6) months from the date of installation unless otherwise required by the specifications of any agreement.

(b) To the extent that Contractor has validated an operating system version, Contractor solutions will support the latest versions of operating systems on which Contractor-provided software functions within twenty-four (24) months from official public release of that operating system version.

Cryptographic Requirements:

(a) Contractor shall document how the cryptographic system supporting the Contractor's products and/or services procured under an applicable agreement protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system as specified by City. This documentation shall include, but not be limited to, the following:

   (i) The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (*e.g.*, Secure Hash Algorithm (SHA)- 256, Advanced Encryption Standard (AES)-128, RSA, and Digital Signature Algorithm (DSA)-2048) that are implemented in the system, and how these methods are to be implemented.

   (ii) The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

(b) Contractor will use only "approved" cryptographic methods as defined in the FIPS 140- 2 Standard when enabling encryption on its products.

6. Coordination of Controls for Remote Access (Requirement R1.2.6)

Contractor shall coordinate with City on all remote access to City's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by City to the extent that such controls are not contrary to Contractor's own security policies. Otherwise parties will mutually agree on methods or remote access that satisfy the security requirements of both parties. Contractor agrees to make available a remote access platform that supports the requirements of NERC CIP-005 R2.4 & R2.5. Requirements for Contractor to provide the alternate method of remote access to the City requires mutual agreement on method and additional fees.

Controls for Remote Access: Contractors that directly, or through any of their affiliates, subcontractors or service providers, connect to City's systems or networks agree to the additional following protective measures:

(a) Contractor will not access and will not permit any other person or entity to access, City's systems or networks without City's authorization and any such actual or attempted access will be consistent with any such authorization.

(b) Contractor shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.

(c) Contractor shall ensure Contractor Personnel do not use any virtual private network or other device to simultaneously connect machines on any City system or network to any machines on any Contractor or third-party systems, without

   (i) providing City with the full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and

(ii) ensuring that any computer used by Contractor Personnel to remotely access any City system or network will not simultaneously access the Internet or any other third-party system or network while logged on to City systems or networks.

(d) Contractor shall ensure Contractor Personnel accessing City networks are uniquely identified and that accounts are not shared between Contractor Personnel.

7. Supporting Provisions

Contractor Cybersecurity Policy: Contractor will provide to City upon request a summary of the Contractor's cybersecurity policy as applicable to the products and services provided, which shall be consistent with ISO-27001 and more broadly with NIST Special Publication 800-53 (Rev. 5) as may be amended. Contractor will implement and comply with Contractor's established cybersecurity policies.

Any material changes to Contractor's cybersecurity policy as applied to products and services provided to City and City Information shall not decrease the protections afforded to City or City Information and any material changes that that Contractor confirms decreases such protections shall be communicated by Contractor.

Return or Destruction of City Information: Upon completion of the delivery of the products and services to be provided under the Services Agreement, or at any time upon City's request, Contractor will return to City all hardware and removable media provided by City containing City Information. City Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by City. If the hardware or removable media containing City Information is owned by Contractor or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated City security representative within thirty (30) calendar days after completion of the delivery of the products and services to be provided under the Agreement, or at any time upon City's request. Contractor's destruction or erasure of City Information pursuant to this Section shall be in compliance with best industry practices (*e.g.*, Department of Defense 5220-22-M Standard, as may be amended).

Notwithstanding the foregoing, City agrees that Contractor shall not be required to return to City, or destroy, copies of City Information that (A) reside on Contractor's backup, disaster recovery or business continuity systems, or (B) that Contractor is obligated by applicable law and/or governmental regulations to retain. Contractor agrees that, following its receipt of the Request, it shall neither retrieve nor use City Information for any purpose other than that specified in clause (B) above.

Audit Rights: Contractor shall follow accepted industry security standards and controls, to the extent Contractor determines applicable. Contractor shall provide to City a copy of its current certification to ISO-27001 standards, along with certain policies & procedures as related to the products and services provided to City and as determined in the sole reasonable judgement of Contractor. Upon request and no more than once per year Contractor will provide a written certification from a certified independent entity that it complies with ISO-27001applicable industry standards, as determined by Contractor's reasonable judgement.

Regulatory Examinations: Contractor shall, upon City's request, promptly cooperate provide all reasonable cooperation with City and will provide any information reasonably requested to support the City's efforts to comply with any examination by a regulator or other governmental entity, and provide all other reasonable assistance requested by the City. Contractor agrees to comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes. Should any recommendations increase costs and/or time for performance the Parties will mutually agree on any applicable changes to the existing Agreement. The assistance required by this paragraph is subject to all confidentiality provisions of this Agreement any applicable protections provided to Contractor under applicable law.

8. **Term.** The "Term" of this Agreement shall commence on the Effective Date, and shall continue in effect until all obligations of the Parties have been met under the Services Agreement and under this Cyber Security Supply Chain Risk Management Agreement.

9. **Termination.** This Agreement may be terminated at any time during its Term upon the mutual written agreement of both Parties. City may terminate immediately this Agreement, and any other related agreements if City makes a determination, in its reasonable opinion, that Contractor has breached a material term of this Agreement and Contractor has failed to cure that material breach, to City's reasonable satisfaction, within 30 days after written notice from City.

10. **No Assignment**. This Agreement shall inure to the benefit of and be binding upon the Parties and their respective successors and permitted assigns. Neither Party shall assign this Agreement or any of its rights or obligations hereunder without the prior written consent of the other Party.

11. **Notices.** Any notice, demand, request, or communication required or authorized by the Agreement shall be delivered either by hand, facsimile, overnight courier or mailed by certified mail, return receipt requested, with postage prepaid, to:

If to City:
City of Columbia
Utilities Department
P.O. Box 6015
Columbia, MO 65205-6015
ATTN: Director

With a copy to:
City of Columbia
Information Technologies Department
P.O. Box 6015
Columbia, MO 65205-6015
ATTN: Director

If to Contractor:
Open Systems International, Inc.
4101 Arrowhead Drive, Medina, Minnesota 55340
ATTN: Ken Hall, Contract Manager

The designation and titles of the person to be notified or the address of such person may be changed at any time by written notice. Any such notice, demand, request, or communication shall be deemed delivered on receipt if delivered by hand or facsimile and on deposit by the sending party if delivered by courier or U.S. mail.

12. **No Third-Party Beneficiary**. No provision of the Agreement is intended to nor shall it in any way inure to the benefit of any other third party, so as to constitute any such Person a third-party beneficiary under the Agreement.

13. **Amendment.** No amendment, addition to, or modification of any provision hereof shall be binding upon the Parties, and neither Party shall be deemed to have waived any provision or any remedy

available to it unless such amendment, addition, modification or waiver is in writing and signed by a duly authorized officer or representative of the applicable Party or Parties.

14. **Governing Law and Venue.** This contract shall be governed, interpreted, and enforced in accordance with the laws of the State of Missouri and/or the laws of the United States, as applicable. The venue for all litigation arising out of, or relating to this contract document, shall be in Boone County, Missouri, or the United States Western District of Missouri. The Parties hereto irrevocably agree to submit to the exclusive jurisdiction of such courts in the State of Missouri. The Parties agree to waive any defense of forum non conveniens.

15. **General Laws.** The Parties shall comply with all applicable federal, state, and local laws, rules, regulations, and ordinances.

16. **No Waiver of Immunities**. In no event shall the language of this Agreement constitute or be construed as a waiver or limitation for either party's rights or defenses with regard to each party's applicable sovereign, governmental, or official immunities and protections as provided by federal and state constitutions or laws.

17. This Agreement may be signed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. Faxed signatures, or scanned and electronically transmitted signatures, on this Agreement or any notice delivered pursuant to this Agreement, shall be deemed to have the same legal effect as original signatures on this Agreement.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the parties have executed this Agreement on the day set forth below each of their signatures.

City of Columbia, Missouri

By: __________________________
De'Carlon Seewood, City Manager DAS

Date: __________________________

ATTEST:

By: __________________________
Sheela Amin, City Clerk

APPROVED AS TO FORM:

By: __________________________
Nancy Thompson, City Counselor/rw

CONTRACTOR:
Open Systems International, Inc.

BY: Albert Eli

PRINTED
NAME: Al Eliasen

TITLE: President

DATE: 2/1/2022

ATTEST:

BY: ____________________

TITLE: ____________________