PROFESSIONAL CONSULTANT SERVICES AGREEMENT (TECHNOLOGY SERVICES)

AESI-US, INC.

CYBER SECURITY PROFESSIONAL CONSULTING SERVICES

THIS PROFESSIONAL CONSULTANT SERVICES AGREEMENT ("Agreement") is made and entered into this _____ day of _____ 2025 ("Effective Date"), by and between the CITY OF RIVERSIDE, a California charter city and municipal corporation ("City"), and AESI-US, INC., a Georgia corporation authorized to do business in California ("Consultant").

1. **Scope of Services**. City agrees to retain and does hereby retain Consultant and Consultant agrees to provide the services more particularly described in Exhibit "A," "Scope of Services" ("Services"), attached hereto and incorporated herein by reference, in conjunction with CYBER SECURITY PROFESSIONAL CONSULTING SERVICES ("Project").

2. **Term**. This Agreement shall be effective on the date first written above and shall remain in effect until three years from the Effective Date, unless otherwise terminated pursuant to the provisions herein.

3. **Compensation/Payment**. Consultant shall perform the Services under this Agreement for the total sum of **Three Hundred Twenty-Nine Thousand One Hundred Dollars** (**$329,100**) payable in accordance with the terms set forth in Exhibit "B." Said payment shall be made in accordance with City's usual accounting procedures upon receipt and approval of an itemized invoice setting forth the services performed. The invoices shall be delivered to City at the address set forth in Section 4 hereof.

4. **Notices**. Any notices required to be given, hereunder shall be in writing and shall be personally served or given by mail. Any notice given by mail shall be deemed given when deposited in the United States Mail, certified and postage prepaid, addressed to the party to be served as follows:

To City	To Consultant
Public Utilities General Manager City of Riverside Attn: David Garcia 3750 University Avenue, 5th Floor Riverside, CA 92501	AESI-US, Inc. Attn: Doug Westlund 412 E. Main Street, Lower Level New Albany, IN 47150

5. **Prevailing Wage**. If applicable, Consultant and all subcontractors are required to pay the general prevailing wage rates of per diem wages and overtime and holiday wages determined by the Director of the Department of Industrial Relations under Section 1720 et seq. of the California Labor Code and implemented by Resolution No. 13346 of the City Council of the City of Riverside. The Director's determination is available on-line at www.dir.ca.gov/dlsr/DPreWageDetermination.htm and is referred to and made a part hereof; the wage rates therein ascertained, determined, and specified are referred to and made a part hereof as though fully set forth herein.

6. **Contract Administration**. A designee of the City will be appointed in writing by the City Manager or Department Director to administer this Agreement on behalf of City and shall be referred to herein as Contract Administrator.

7. **Standard of Performance**. While performing the Services, Consultant shall exercise the reasonable professional care and skill customarily exercised by reputable members of Consultant's profession practicing in the Metropolitan Southern California Area, and shall use reasonable diligence and best judgment while exercising its professional skill and expertise.

8. **Personnel**. Consultant shall furnish all personnel necessary to perform the Services and shall be responsible for their performance and compensation. Consultant recognizes that the qualifications and experience of the personnel to be used are vital to professional and timely completion of the Services. The key personnel listed in Exhibit "C" attached hereto and incorporated herein by this reference and assigned to perform portions of the Services shall remain assigned through completion of the Services, unless otherwise mutually agreed by the parties in writing, or caused by hardship or resignation in which case substitutes shall be subject to City approval.

9. **Assignment and Subcontracting**. Neither party shall assign any right, interest, or obligation in or under this Agreement to any other entity without prior written consent of the other party. In any event, no assignment shall be made unless the assignee expressly assumes the obligations of assignor under this Agreement, in a writing satisfactory to the parties. Consultant acknowledges that any assignment may, at the City's sole discretion, require City Manager and/or City Council approval. Consultant shall not subcontract any portion of the work required by this Agreement without prior written approval by the responsible City Contract Administrator. Subcontracts, if any, shall contain a provision making them subject to all provisions stipulated in this Agreement, including without limitation, the insurance obligations set forth in Section 12. The Consultant acknowledges and agrees that the City is an intended beneficiary of any work performed by any subcontractor for purposes of establishing a duty of care between any subcontractor and the City.

10. **Independent Contractor**. In the performance of this Agreement, Consultant, and Consultant's employees, subcontractors and agents, shall act in an independent capacity as independent contractors, and not as officers or employees of the City of Riverside. Consultant acknowledges and agrees that the City has no obligation to pay or withhold state or federal taxes or to provide workers' compensation or unemployment insurance to Consultant, or to Consultant's employees, subcontractors and agents. Consultant, as an independent contractor, shall be responsible for any and all taxes that apply to Consultant as an employer.

11. **Indemnification**.

11.1 **Design Professional Defined**. For purposes of this Agreement, "Design Professional" includes the following:

A. An individual licensed as an architect pursuant to Chapter 3 (commencing with Section 5500) of Division 3 of the Business and Professions Code, and a business entity offering architectural services in accordance with that chapter.

B. An individual licensed as a landscape architect pursuant to Chapter 3.5 (commencing with Section 5615) of Division 3 of the Business and Professions Code, and a business entity offering landscape architectural services in accordance with that chapter.

C. An individual registered as a professional engineer pursuant to Chapter 7 (commencing with Section 6700) of Division 3 of the Business and Professions Code, and a business entity offering professional engineering services in accordance with that chapter.

D. An individual licensed as a professional land surveyor pursuant to Chapter 15 (commencing with Section 8700) of Division 3 of the Business and Professions Code, and a business entity offering professional land surveying services in accordance with that chapter.

11.2 **Defense Obligation For Design Professional Liability**. Consultant agrees, at its cost and expense, to promptly defend the City, and the City's employees, officers, managers, agents and council members (collectively the "Parties to be Defended") from and against any and all claims, allegations, lawsuits, arbitration proceedings, administrative proceedings, regulatory proceedings, or other legal proceedings to the extent the same arise out of, pertain to, or relate to the negligence, recklessness or willful misconduct of Consultant, or anyone employed by or working under the Consultant or for services rendered to the Consultant in the performance of the Agreement, notwithstanding that the City may have benefited from its work or services and whether or not caused in part by the negligence of an Indemnified Party. Consultant agrees to provide this defense immediately upon written notice from the City, and with well qualified, adequately insured and experienced legal counsel acceptable to City. Consultant will reimburse City for reasonable defense costs for claims arising out of Consultant's professional negligence based on the percentage of Consultant's liability. This obligation to defend as set forth herein is binding on the successors, assigns and heirs of Consultant and shall survive the termination of Consultant's Services under this Agreement.

11.3 **Indemnity For Design Professional Liability**. When the law establishes a professional standard of care for Consultant's services, to the fullest extent permitted by law, Consultant shall indemnify, protect and hold harmless the City and the City's employees, officers, managers, agents, and Council Members ("Indemnified Parties") from and against any and all claim for damage, charge, lawsuit, action, judicial, administrative, regulatory or arbitration proceeding, damage, cost, expense (including counsel and expert fees), judgment, civil fines and

penalties, liabilities or losses of any kind or nature whatsoever to the extent the same arise out of, pertain to, or relate to the negligence, recklessness or willful misconduct of Consultant, or anyone employed by or working under the Consultant or for services rendered to the Consultant in the performance of the Agreement, notwithstanding that the City may have benefited from its work or services and whether or not caused in part by the negligence of an Indemnified Party.

11.4 **Defense Obligation For Other Than Design Professional Liability**. Consultant agrees, at its cost and expense, to promptly defend the City, and the City's employees, officers, managers, agents and council members (collectively the "Parties to be Defended") from and against any and all claims, allegations, lawsuits, arbitration proceedings, administrative proceedings, regulatory proceedings, or other legal proceedings which arise out of, or relate to, or are in any way connected with: 1) the Services, work, activities, operations, or duties of the Consultant, or of anyone employed by or working under the Consultant, or 2) any breach of the Agreement by the Consultant. This duty to defend shall apply whether or not such claims, allegations, lawsuits or proceedings have merit or are meritless, or which involve claims or allegations that any or all of the Parties to be Defended were actively, passively, or concurrently negligent, or which otherwise assert that the Parties to be Defended are responsible, in whole or in part, for any loss, damage or injury. Consultant agrees to provide this defense immediately upon written notice from the City, and with well qualified, adequately insured and experienced legal counsel acceptable to City. This obligation to defend as set forth herein is binding on the successors, assigns and heirs of Consultant and shall survive the termination of Consultant's Services under this Agreement.

11.5 **Indemnity For Other Than Design Professional Liability**. Except as to the sole negligence or willful misconduct of the City, Consultant agrees to indemnify, protect and hold harmless the Indemnified Parties from and against any claim for damage, charge, lawsuit, action, judicial, administrative, regulatory or arbitration proceeding, damage, cost, expense (including counsel and expert fees), judgment, civil fine and penalties, liabilities or losses of any kind or nature whatsoever whether actual, threatened or alleged, which arise out of, pertain to, or relate to, or are a consequence of, or are attributable to, or are in any manner connected with the performance of the Services, work, activities, operations or duties of the Consultant, or anyone employed by or working under the Consultant or for services rendered to Consultant in the performance of this Agreement, notwithstanding that the City may have benefited from its work or services. This indemnification provision shall apply to any acts, omissions, negligence, recklessness, or willful misconduct, whether active or passive, on the part of the Consultant or anyone employed or working under the Consultant.

12. **Insurance**.

12.1 **General Provisions**. Prior to the City's execution of this Agreement, Consultant shall provide satisfactory evidence of, and shall thereafter maintain during the term of this Agreement, such insurance policies and coverages in the types, limits, forms and ratings required herein. The rating and required insurance policies and coverages may be modified in writing by the City's Risk Manager or City Attorney, or a designee, unless such modification is prohibited by law.

12.1.1 **Limitations**. These minimum amounts of coverage shall not constitute any limitation or cap on Consultant's indemnification obligations under Section 11 hereof.

12.1.2 **Ratings**. Any insurance policy or coverage provided by Consultant or subcontractors as required by this Agreement shall be deemed inadequate and a material breach of this Agreement, unless such policy or coverage is issued by insurance companies authorized to transact insurance business in the State of California with a policy holder's rating of A or higher and a Financial Class of VII or higher.

12.1.3 **Cancellation**. The policies shall not be canceled unless thirty (30) days' prior written notification of intended cancellation has been given to City by certified or registered mail, postage prepaid.

12.1.4 **Adequacy**. The City, its officers, employees and agents make no representation that the types or limits of insurance specified to be carried by Consultant pursuant to this Agreement are adequate to protect Consultant. If Consultant believes that any required insurance coverage is inadequate, Consultant will obtain such additional insurance coverage as Consultant deems adequate, at Consultant's sole expense.

12.2 **Workers' Compensation Insurance**. By executing this Agreement, Consultant certifies that Consultant is aware of and will comply with Section 3700 of the Labor Code of the State of California requiring every employer to be insured against liability for workers' compensation, or to undertake self-insurance before commencing any of the work. Consultant shall carry the insurance or provide for self-insurance required by California law to protect said Consultant from claims under the Workers' Compensation Act. Prior to City's execution of this Agreement, Consultant shall file with City either 1) a certificate of insurance showing that such insurance is in effect, or that Consultant is self-insured for such coverage, or 2) a certified statement that Consultant has no employees, and acknowledging that if Consultant does employ any person, the necessary certificate of insurance will immediately be filed with City. Any certificate filed with City shall provide that City will be given ten (10) days' prior written notice before modification or cancellation thereof.

12.3 **Commercial General Liability and Automobile Insurance**. Prior to City's execution of this Agreement, Consultant shall obtain, and shall thereafter maintain during the term of this Agreement, commercial general liability insurance and automobile liability insurance as required to insure Consultant against damages for personal injury, including accidental death, as well as from claims for property damage, which may arise from or which may concern operations by anyone directly or indirectly employed by, connected with, or acting for or on behalf of Consultant. The City, and its officers, employees and agents, shall be named as additional insureds under the Consultant's insurance policies.

12.3.1 Consultant's commercial general liability insurance policy shall cover both bodily injury (including death) and property damage (including, but not limited to, premises operations liability, products-completed operations liability, independent contractor's liability, personal injury liability, and contractual liability) in an amount not less than $1,000,000 per occurrence and a general aggregate limit in the amount of not less than $2,000,000.

12.3.2 Consultant's automobile liability policy shall cover both bodily injury and property damage in an amount not less than $1,000,000 per occurrence and an aggregate limit of not less than $1,000,000. All of Consultant's automobile and/or commercial general liability insurance policies shall cover all vehicles used in connection with Consultant's performance of this Agreement, which vehicles shall include, but are not limited to, Consultant owned vehicles, Consultant leased vehicles, Consultant's employee vehicles, non-Consultant owned vehicles and hired vehicles.

12.3.3 Prior to City's execution of this Agreement, copies of insurance policies or original certificates along with additional insured endorsements acceptable to the City evidencing the coverage required by this Agreement, for both commercial general and automobile liability insurance, shall be filed with City and shall include the City and its officers, employees and agents, as additional insureds. Said policies shall be in the usual form of commercial general and automobile liability insurance policies, but shall include the following provisions:

> It is agreed that the City of Riverside, and its officers, employees and agents, are added as additional insureds under this policy, solely for work done by and on behalf of the named insured for the City of Riverside.

12.3.4 The insurance policy or policies shall also comply with the following provisions:

a. The policy shall be endorsed to waive any right of subrogation against the City and its sub-consultants, employees, officers and agents for services performed under this Agreement.

b. If the policy is written on a claims made basis, the certificate should so specify and the policy must continue in force for one year after completion of the services. The retroactive date of coverage must also be listed.

c. The policy shall specify that the insurance provided by Consultant will be considered primary and not contributory to any other insurance available to the City and Endorsement No. CG 20010413 shall be provided to the City.

12.4 **Errors and Omissions Insurance**. Prior to City's execution of this Agreement, Consultant shall obtain, and shall thereafter maintain during the term of this Agreement, errors and omissions professional liability insurance in the minimum amount of $1,000,000 to protect the City from claims resulting from the Consultant's activities.

12.5 **Subcontractors' Insurance**. Consultant shall require all of its subcontractors to carry insurance, in an amount sufficient to cover the risk of injury, damage or loss that may be caused by the subcontractors' scope of work and activities provided in furtherance of this Agreement, including, but without limitation, the following coverages: Workers Compensation, Commercial General Liability, Errors and Omissions, and Automobile liability.

Upon City's request, Consultant shall provide City with satisfactory evidence that Subcontractors have obtained insurance policies and coverages required by this section.

12.6 **Technology Professional Liability**. Prior to City's execution of this Agreement, Consultant shall obtain and maintain during the term of this Agreement technology errors and omissions professional liability insurance with limits not less than $1,000,000 per occurrence or claim, $1,000,000 aggregate, to protect the City from claims resulting from the Consultant's professional services as described specifically herein. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

12.7. **Cyber Liability Insurance**. Prior to City's execution of this Agreement, Consultant shall obtain and maintain during the term of this Agreement cyber liability insurance with limits not less than $1,000,000 per occurrence or claim, $1,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

13. **Business Tax**. Consultant understands that the Services performed under this Agreement constitutes doing business in the City of Riverside, and Consultant agrees that Consultant will register for and pay a business tax pursuant to Chapter 5.04 of the Riverside Municipal Code and keep such tax certificate current during the term of this Agreement.

14. **Time of Essence**. Time is of the essence for each and every provision of this Agreement.

15. **City's Right to Employ Other Consultants**. City reserves the right to employ other Consultants in connection with the Project. If the City is required to employ another consultant to complete Consultant's work, due to the failure of the Consultant to perform, or due to the breach of any of the provisions of this Agreement, the City reserves the right to seek reimbursement from Consultant.

16. **Accounting Records**. Consultant shall maintain complete and accurate records with respect to costs incurred under this Agreement. All such records shall be clearly identifiable. Consultant shall allow a representative of City during normal business hours to examine, audit, and make transcripts or copies of such records and any other documents created pursuant to this Agreement. Consultant shall allow inspection of all work, data, documents, proceedings, and

activities related to the Agreement for a period of three (3) years from the date of final payment under this Agreement.

17. **Confidentiality**. All ideas, memoranda, specifications, plans, procedures, drawings, descriptions, computer program data, input record data, written information, and other materials either created by or provided to Consultant in connection with the performance of this Agreement shall be held confidential by Consultant, except as otherwise directed by City's Contract Administrator. Nothing furnished to Consultant which is otherwise known to the Consultant or is generally known, or has become known, to the related industry shall be deemed confidential. Consultant shall not use City's name or insignia, photographs of the Project, or any publicity pertaining to the Services or the Project in any magazine, trade paper, newspaper, television or radio production, website, or other similar medium without the prior written consent of the City.

18. **Ownership of Documents**. All reports, maps, drawings and other contract deliverables prepared under this Agreement by Consultant shall be and remain the property of City. Consultant shall not release to others information furnished by City without prior express written approval of City.

19. **Copyrights.** Consultant agrees that any work prepared for City which is eligible for copyright protection in the United States or elsewhere shall be a work made for hire. If any such work is deemed for any reason not to be a work made for hire, Consultant assigns all right, title and interest in the copyright in such work, and all extensions and renewals thereof, to City, and agrees to provide all assistance reasonably requested by City in the establishment, preservation and enforcement of its copyright in such work, such assistance to be provided at City's expense but without any additional compensation to Consultant. Consultant agrees to waive all moral rights relating to the work developed or produced, including without limitation any and all rights of identification of authorship and any and all rights of approval, restriction or limitation on use or subsequent modifications.

20. **Conflict of Interest**. Consultant, for itself and on behalf of the individuals listed in Exhibit "C," represents and warrants that by the execution of this Agreement, they have no interest, present or contemplated, in the Project affected by the above-described Services. Consultant further warrants that neither Consultant, nor the individuals listed in Exhibit "C" have any real property, business interests or income interests that will be affected by this project or, alternatively, that Consultant will file with the City an affidavit disclosing any such interest.

21. **Solicitation**. Consultant warrants that Consultant has not employed or retained any person or agency to solicit or secure this Agreement, nor has it entered into any agreement or understanding for a commission, percentage, brokerage, or contingent fee to be paid to secure this Agreement. For breach of this warranty, City shall have the right to terminate this Agreement without liability and pay Consultant only for the value of work Consultant has actually performed, or, in its sole discretion, to deduct from the Agreement price or otherwise recover from Consultant the full amount of such commission, percentage, brokerage or commission fee. The remedies specified in this section shall be in addition to and not in lieu of those remedies otherwise specified in this Agreement.

22. **General Compliance with Laws**. Consultant shall keep fully informed of federal, state and local laws and ordinances and regulations which in any manner affect those employed by Consultant, or in any way affect the performance of services by Consultant pursuant to this Agreement. Consultant shall at all times observe and comply with all such laws, ordinances and regulations, and shall be solely responsible for any failure to comply with all applicable laws, ordinances and regulations. Consultant represents and warrants that Consultant has obtained all necessary licenses to perform the Scope of Services and that such licenses are in good standing. Consultant further represents and warrants that the services provided herein shall conform to all ordinances, policies and practices of the City of Riverside.

23. **Waiver**. No action or failure to act by the City shall constitute a waiver of any right or duty afforded City under this Agreement, nor shall any such action or failure to act constitute approval of or acquiescence in any breach thereunder, except as may be specifically, provided in this Agreement or as may be otherwise agreed in writing.

24. **Amendments**. This Agreement may be modified or amended only by a written agreement and/or change order executed by the Consultant and City.

25. **Termination**. City, by notifying Consultant in writing, shall have the right to terminate any or all of Consultant's services and work covered by this Agreement at any time. In the event of such termination, Consultant may submit Consultant's final written statement of the amount of Consultant's services as of the date of such termination based upon the ratio that the work completed bears to the total work required to make the report complete, subject to the City's rights under Sections 15 and 26 hereof. In ascertaining the work actually rendered through the termination date, City shall consider completed work, work in progress and complete and incomplete reports and other documents only after delivered to City.

25.1 Other than as stated below, City shall give Consultant thirty (30) days' prior written notice prior to termination.

25.2 City may terminate this Agreement upon fifteen (15) days' written notice to Consultant, in the event:

25.2.1 Consultant substantially fails to perform or materially breaches the Agreement; or

25.2.2 City decides to abandon or postpone the Project.

26. **Offsets**. Consultant acknowledges and agrees that with respect to any business tax or penalties thereon, utility charges, invoiced fee or other debt which Consultant owes or may owe to the City, City reserves the right to withhold and offset said amounts from payments or refunds or reimbursements owed by City to Consultant. Notice of such withholding and offset, shall promptly be given to Consultant by City in writing. In the event of a dispute as to the amount owed or whether such amount is owed to the City, City will hold such disputed amount until either the appropriate appeal process has been completed or until the dispute has been resolved.

27. **Successors and Assigns**. This Agreement shall be binding upon City and its successors and assigns, and upon Consultant and its permitted successors and assigns, and shall

not be assigned by Consultant, either in whole or in part, except as otherwise provided in paragraph 9 of this Agreement.

28. **Venue.** Any action at law or in equity brought by either of the parties hereto for the purpose of enforcing a right or rights provided for by this Agreement shall be tried in a court of competent jurisdiction in the County of Riverside, State of California, and the parties hereby waive all provisions of law providing for a change of venue in such proceedings to any other county. In the event either party hereto shall bring suit to enforce any term of this Agreement or to recover any damages for and on account of the breach of any term or condition of this Agreement, it is mutually agreed that each party will bear their own attorney's fees and costs.

29. **Nondiscrimination**. During Consultant's performance of this Agreement, Consultant shall not discriminate on the grounds of race, religious creed, color, national origin, ancestry, age, physical disability, mental disability, medical condition, including the medical condition of Acquired Immune Deficiency Syndrome (AIDS) or any condition related thereto, marital status, sex, genetic information, gender, gender identity, gender expression, or sexual orientation, military and veteran status, in the selection and retention of employees and subcontractors and the procurement of materials and equipment, except as provided in Section 12940 of the California Government Code. Further, Consultant agrees to conform to the requirements of the Americans with Disabilities Act in the performance of this Agreement.

30. **Severability**. Each provision, term, condition, covenant and/or restriction, in whole and in part, of this Agreement shall be considered severable. In the event any provision, term, condition, covenant and/or restriction, in whole and/or in part, of this Agreement is declared invalid, unconstitutional, or void for any reason, such provision or part thereof shall be severed from this Agreement and shall not affect any other provision, term, condition, covenant and/or restriction of this Agreement, and the remainder of the Agreement shall continue in full force and effect.

31. **Authority**. The individuals executing this Agreement and the instruments referenced herein on behalf of Consultant each represent and warrant that they have the legal power, right and actual authority to bind Consultant to the terms and conditions hereof and thereof.

32. **Entire Agreement**. This Agreement constitutes the final, complete, and exclusive statement of the terms of the agreement between the parties pertaining to the subject matter of this Agreement, and supersedes all prior and contemporaneous understandings or agreements of the parties. Neither party has been induced to enter into this Agreement by and neither party is relying on, any representation or warranty outside those expressly set forth in this Agreement.

33. **Digital and Counterpart Signatures**. Each party to this Agreement intends and agrees to the use of digital signatures that meets the requirements of the California Uniform Electronic Transactions Act (Civil Code §§ 1633.1, et seq.), California Government Code § 16.5, and California Code of Regulations Title 2 Division 7 Chapter 10, to execute this Agreement. The parties further agree that the digital signatures of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures for purposes of validity, enforceability, and admissibility. For purposes of this section, a "digital signature" is defined in subdivision (d) of Section 16.5 of the Government Code and is a type of

"electronic signature" as defined in subdivision (h) of Section 1633.2 of the Civil Code. This Agreement may be executed in any number of counterparts, each of which will be an original, but all of which together will constitute one instrument. Each certified or authenticated electronic copy of an encrypted digital signature shall be deemed a duplicate original, constituting one and the same instrument and shall be binding on the parties hereto.

34. **Interpretation**. City and Consultant acknowledge and agree that this Agreement is the product of mutual arms-length negotiations and accordingly, the rule of construction, which provides that the ambiguities in a document shall be construed against the drafter of that document, shall have no application to the interpretation and enforcement of this Agreement.

34.1 Titles and captions are for convenience of reference only and do not define, describe or limit the scope or the intent of the Agreement or any of its terms. Reference to section numbers, are to sections in the Agreement unless expressly stated otherwise.

34.2 This Agreement shall be governed by and construed in accordance with the laws of the State of California in effect at the time of the execution of this Agreement.

34.3 In the event of a conflict between the body of this Agreement and Exhibit "A" - Scope of Services hereto, the terms contained in Exhibit "A" shall be controlling.

35. **Exhibits**. The following exhibits attached hereto are incorporated herein to this Agreement by this reference:

Exhibit "A" - Scope of Services
Exhibit "B" - Compensation
Exhibit "C" - Key Personnel

IN WITNESS WHEREOF, City and Consultant have caused this Agreement to be duly executed the day and year first above written.

CITY OF RIVERSIDE, a California charter city and municipal corporation

By: _____
City Manager

Attest: _____
City Clerk

Certified as to Availability of Funds:

By: _____
Chief Financial Officer

Approved as to Form:

By: _____
Senior Deputy City Attorney

AESI-US, INC., a Georgia corporation authorized to do business in California

By: JCharlebois
JCharlebois (Jan 13, 2025 19:08 GMT)

Joel Charlebois, P. Eng

Vice President

By: _____

[Printed Name]

[Title]

EXHIBIT "A"

SCOPE OF SERVICES

1. OT Cyber Program Assessment

A) Review the network architecture, security controls, policies, facilities and organization to identify gaps and mitigation solutions for Critical Infrastructure Protection of each identified OT system within Riverside public utilities Electric Generation, Distribution, Water, Substation and Fiber optic operational technology isolated infrastructure. Provide documentation of the assessment for each system in alignment with the NIST Cyber Security Framework/NERC CIP Reliability Standards, including:

i.) OT System Identification and Categorization, including but not limited to

   a) RTUs, PLCs, HMIs, PCs, Laptops, LMR systems, safety, and monitoring systems, switches, routers, firewalls, Servers, and software within the OT-isolated segments.

ii.) Security Management Controls
iii.) Personnel and Training
iv.) Electronic Security Perimeter including but not limited to OT – City demilitarized zone, OT partner connectivity such as CAISO or other ingress or egress channels to Riverside public utilities OT infrastructure
v.) Physical Security of OT Systems and Facilities
vi.) System Security Management
vii.) Incident Reporting and Response Training
viii.) Recovery Planning for OT Systems
ix.) Configuration Change Management and Vulnerability Assessments
x.) Information Protection
xi.) Supply Chain Risk Management
xii.) Identity and access management
xiii.) Shared accounts, password management practices, and risk exposure from separated employees or consultants.
xiv.) Separation of duties and role-based access control
xv.) Least privilege architecture
xvi.) Insider threat assessment, including security screening, monitoring, abnormal activity detection, and management oversight.
xvii.) Remote and field access to OT / SCADA networks mentioned in section 1, A, i

Mitigation Plans should identify recommended improvements, budgetary cost estimate, proposed schedule and priority for implementation to minimize exposure and impact.

B) Continuous monitoring and scanning program development with emphasis on non-disruptive processes to avoid OT service disruptions

i.) External
ii.) Internal
iii.) Authenticated/Unauthenticated

C) Patching and vulnerability program development or review

D) Change management review

E) Review of external entities and service providers

i.) Review of inherited risk based on vendor and service agreements
ii.) Supply Chain / interdiction review and advisement

2. OT Cyber Posture Assessments

A) Evaluation of organization ability to protect information and systems

B) Open Source Intelligence (OSINT) review of an organization

i.) Reconnaissance
ii.) Existing data exfiltration issues
iii.) Identification of existing OSINT attack risks and vectors
iv.) Sanitization and sterilization of existing OSINT
v.) Cyber posture portfolio creation
vi.) Social media presence and risk acceptance

C) Complete exposure and risk profile with mitigation recommendations

D) Real-world attack simulation and assessment

E) Cyber components of physical system assessment

i.) RFID readers
ii.) Door locks
iii.) Barriers
iv.) Physical Access Systems (PACs)

F) Personnel Security Assessment

3. OT environments Vulnerability Assessment Services

A) System scanning

i.) OT, SCADA, PACs, proprietary
ii.) Scan result analysis assistance
iii.) Manual scanning services

a) Production environment considerations
b) Automated scanning enhancement

B) Verification of system and network interconnections and/or isolation

C) Risk analysis of critical systems via vulnerability identification

D) Code review

E) Identification and classification of vulnerabilities across organizational infrastructure

F) Vulnerability remediation advisement

i.) Critical systems considerations
ii.) Risk acceptance analysis

4. OT environments Penetration Testing Services

i.) Full scope penetration tests
ii.) Cyber asset enumeration
iii.) Exploitation validation tests
iv.) External OT network penetration tests
v.) Insider threat penetration tests
vi.) Phishing and spear Phishing attack campaigns of OT staff
vii.) OT control systems Wireless penetration tests
viii.) Announced penetration tests
ix.) SCADA systems penetration testing
x.) Advanced Persistence Threat tests (APTs)
xi.) Intrusion Detection System (IDS) and firewall penetration testing services
xii.) Exfiltration awareness tests
xiii.) NOC/SOC testing and advisement engagements
xiv.) Physical penetration tests
xv.) Social Engineering penetration tests

5. OT Remediation Services

i.) System baseline establishment and verification
ii.) Patching and upgrading planning and implementation
iii.) Risk mitigation strategies for legacy systems
iv.) Programmatic policy and procedure creation and/or analysis
v.) Post incident response remediation analysis
vi.) NOC/SOC management service
vii.) Third party vendor risk mitigation services
viii.) Legacy system attrition plan development
ix.) Backup and recovery testing and validation

6. OT Incident Response Services

A) Provide range of services to identify emerging cyber and physical threats to OT Systems, preventive measures, incident detection, containment, and recovery. Services may be provided directly, or through mutual assistance, contract services, or governmental assistance. Incident reporting requirements and response time frames should be clearly identified.

i.) Cyber event identification
ii.) Active cyber event containment
iii.) Cyber event investigations
iv.) Forensic analysis post cyber event
v.) Post cyber event actions
vi.) Tabletop IR activities
vii.) Active cyber event mitigation
viii.) OSINT control and containment of cyber events

7. In-Person Training Services

A) Conduct regular on-site or webinar meetings with the RPU Cyber Information Security Team, including OT System Administrators, technical staff, system operators and compliance manager. Discuss emerging issues, recommend mitigation/prevention, evaluate incidents, address changes related to NERC CIP/NIST guidance. Provide an agenda and minutes to document action items.

i.) Onsite training courses
ii.) Development of organization specific training courses (as requested)
iii.) Tool specific training courses
iv.) Subject matter expert training courses
v.) Hands on training for employees in their own environments
vi.) Knowledge assessment testing for critical personnel
vii.) Software specific training courses
viii.) Secure coding training
ix.) Basic security training for non-technical employees (not already provided by City IT)

a) Social media security risks and considerations
b) Security best practices
c) Social engineering defensive training

8. One-On-One Mentoring Services

A) Direct, one-on-one training

B) Tailored training for critical personnel

C) Subject matter expert training

D) Full-scope training for administrators

E) Co-development services

9. Laboratory Training Services

A) Laboratory training in environments that mirror customer systems

B) Full complement of technical training environments
   i.) Networks
   ii.) SCADA
   iii.) IT
   iv.) OT
   v.) IOT
   vi.) PACs
   vii.) PLCs
   viii.) HMIs
   ix.) SIEM

C) Physical installation training

D) Full OSI model training

E) Real-time exercise training

F) Blue team training

G) Red team training

10. Budget Scope

A) Review the scope of proposed Capital Improvement Plan Budget projects to verify that all OT System Assessment mitigation items are included and properly specified. Recommend revisions, if needed to implement identified OT System mitigation capital projects.

B) Review the scope of proposed Operating Budget projects to verify that all OT System Assessment mitigation items are included and properly specified. Recommend revisions, if needed to implement identified OT System mitigation projects. Operating budgets typically include personnel, software licenses and updates, equipment maintenance, training and other expenses related to OT Systems.

11. Exercise Services

A) Provide tabletop exercises in conjunction with training to test the effectiveness of training and processes/procedures developed during the Architecture Assessment phase. Conduct after action reviews to identify strengths, weaknesses, opportunities and threats revealed by the tabletop exercise. Identify process/procedure/training revisions necessary to address deficiencies.

B) Provide functional or full-scale exercises (six months after tabletop exercise) to test effectiveness of training and processes/procedures developed during the Architecture Assessment phase. Conduct after action reviews to identify strengths, weaknesses, opportunities, and threats revealed by the functional or full-scale exercise. Identify process/procedure/training revisions necessary to address deficiencies.

12. Confidential RPU General Manager, CIO, CISO, and City Manager's team report of findings and recommendations.

EXHIBIT "B"

COMPENSATION

Item # (Section 2.2)	Item Description	UOM	Hourly Rate	Estimated Hours	Total Labor Cost (a)	Expenses (b)	Total Amount (a+b)
1	Cyber Program Assessment (Also includes items, 2.2.2.1, 2.2.2.2, 2.2.2.4, and 2.2.2.7)	LS	$396	112	$44,200	$4,000	$48,200
2	Cyber Posture Assessments	LS	$290	12	$3,400	$1,900	$5,300
3	Vulnerability Assessment Services	LS	$302	85	$25,800	$2,600	$28,400
4	Penetration Testing Services (Also includes items, 2.2.2.3 and 2.2.2.5)	LS	$307	89	$27,400	$2,200	$29,600
5	Remediation Services	LS	$297	23	$6,700	$0	$6,700

6	Incident Response Services	LS	$297	23	$6,700	$0	$6,700
7	In-Person Training Services	LS	$340	38	$13,000	$2,600	$15,600
8	One-On-One Mentoring Services	LS	$333	53	$17,600	$0	$17,600
9	Laboratory Training Services	LS	$0	20	$0	$0	$0
10	Budget Scoping Services	LS	$414	24	$10,100	$0	$10,100
11	Exercise Services	LS	$341	27	$9,060	$1,840	$10,900
	Grand Total Amount				**$163,960**	**$15,140**	**$179,100**

Notes: For Scope Item #9, Laboratory Training Services, Acumen will be providing 20 hours of facilitation services to RPU at no cost to reinforce our relationship and show our dedication to your success.

This quote stipulates that the total expenditure for incidentals shall not exceed an additional $50,000 per year. All charges related to incidentals will be billed at the agreed-upon hourly rates specified in the quote. Furthermore, no additional work or expenses beyond the defined scope of the agreement shall be undertaken without the prior explicit written authorization of the Project Manager.

Our quote does not include any applicable taxes. Payment is net 30 days with any late payments charged interest at a rate of 1% per month (12.86% per annum) on outstanding balances.

All items have been scoped according to the RFP requirements, including effort and expenses. Any out- of-scope or additional requests will result in adjusted pricing to reflect labor and expenses. Expenses for travel and accommodations will be presented on a best effort estimate and charged as actual costs on a flow through basis, with no administrative markups.

Hourly Rates

Staff	2024 Hourly Rate *
Principal Consultant	$ 415
Senior Executive Consultant	$ 355
Executive Consultant	$ 335
Director/Specialist	$ 315
Senior Consultant II	$ 290
Senior Consultant	$ 265
Consultant II	$ 245
Consultant I	$ 225
Sr. Analyst	$ 195
Sr. Admin	$ 115

* Acumen adjusts its rates annually effective January 1

EXHIBIT "C"

KEY PERSONNEL

Doug Westlund, MBA, P. Eng.

Doug Westlund has more than 35 years of experience in cyber security and operational and IT technology in the utility and telecommunications markets. Doug has extensive experience with the NIST Cyber Security Framework and the NIST Risk Management Framework, having developed a complete risk assessment methodology complete with knowledge transfer and tools that are provided to clients. Doug was the lead developer of the Ontario Cyber Security Framework, a mandatory cyber security compliance framework for Ontario's electric distribution utilities, which is showcased on the NIST resources web page at https://www.nist.gov/cyberframework/critical-infrastructure-resources. Doug provides Board and Executive cyber security and governance training to public power entities via the APPA Academy and was recently the Vice Chair of APPA's Cybersecurity & IT Corporate Council. Doug is a recognized industry leader in cyber security and maintains strong relationships with leading technology, industry and government organizations.

Relevant Experience:

- 150+ cyber security projects in municipal environments with power, water, ISP, city operations, and the co-op sector. These include risk assessments, governance, cyber program development, and a multi-year roadmap for implementation
- Conducting training with multiple Public Power Executive Management Teams and Boards on cyber security as it pertains to utilities, their roles and responsibilities, and the APPA Scorecard - this training is provided by the APPA as a formal APPA Academy training program
- Prime contact for the Hometown Connections partnership and approximately 10 years working with Hometown and the APPA on solving public power challenges
- Developed holistic Cyber Security Blueprint to guide planning, budgeting and implementation efforts for Cyber Security programs for utilities

- Developed methodology to assess the potential financial impact of cyber breaches to provide clients with financial quantification of cyber breaches and an assessment of the residual risk protection from their cyber insurance policies
- Developed risk-based methodology to assess and mitigate the risk associated with supply chain / third parties, i.e., the new number one cyber risk to critical infrastructure entities
- Led the Acumen project team on both the Missouri Joint Municipal Electric Utility Commission (Missouri Public Utility Alliance) and Rochelle Municipal Utilities engagement, both of which included a cyber risk assessment of their operations, integration of APPA Scorecard into the recommendations, prioritized risk-based recommendations, cyber program framework and long-term roadmap
- Led the Acumen project team on 40+ NIST Cybersecurity Framework projects

License, Certifications and Contact Information:

- Contact: **E:** dougw@aesi-inc.com **P:** 770.870.1630 x. 278
- MBA, Ivey School of Business, University of Western Ontario, 1989
- B.A.Sc. in Engineering (Process Control), University of Waterloo, 1984
- Professional Engineers of Ontario (PEO)

Ivan Wong – Cyber Security SME

Ivan is a goal-oriented and collaborative IT professional with more than 15 years of proven experience analyzing and troubleshooting large corporate networks. His utility experience includes NERC CIP compliance support, cyber security vulnerability assessments, mock audits, gap assessments, asset inventory projects, and firewall design/implementation to meet CIP requirements. His strong technical knowledge and ability to quickly learn new systems allow him to provide practical solutions. He is capable of supporting both technical and non-technical audiences.

Relevant Experience:

- Conducted multiple cyber security vulnerability assessments for power generation utilities, distribution utilities, water treatment plants, and corporate environments through preliminary document review, on-site vulnerability scans, and analysis
- Worked at Hydro One in Ontario on their NERC Compliance team
- Implemented cyber security tools, such as firewalls, access controls, SIEM, and network monitoring tools at client sites to meet CIP requirements
- Participated in developing clear, concise and effective NERC CIP Compliance Program policies, procedures and compliance gathering processes, templates and other aids
- Designed and implemented firewalls that met NERC CIP v3 and v5 requirements for power generation and distribution utilities

- Provided network services to power generation and distribution utilities, including configuration review, network troubleshooting, network design, network implementation, access rules review, and network diagrams creation
- Reviewed and updated compliance documentation to ensure it meets NERC CIP requirements
- Identified non-compliance items and created Self-Reports for submission
- Conducted wireless assessments at client sites, identifying rogue access points and ensuring best security practices were used
- Conducted Cyber Asset Inventories for Control Centers, generating and transmission facilities
- Designed electronic access controls for generating and transmission facilities to control electronic access
- Developed IT/OT cyber security training for American Public Power Association (APPA)
- Managed and participated in NERC audits for CIP Compliance review, such that Acumen has sufficient information on their OT system to be able to provide support in the event of any Cyber Security Incidents
- Helped utilities in reviewing and providing improvements in their Disaster Planning and Recovery
- Supported Utilities in actual disaster recovery
- Participated in forensic security audits

License, Certifications and Contact Information:

- Contact: **E:** ivanw@aesi-inc.com **P:** 770.870.1630 x. 261
- Bachelor of Engineering, Electrical Engineering, Ryerson University, Toronto, 2008
- Cisco Certified Network Associate – CCNA (CSCO11964943)
- VMware – VCP6-DCV
- Cisco Certified Network Associate – CCNA, 2011
- Cisco Certified Network Associate Voice – CCNA Voice, 2012
- Cisco Certified Network Associate Wireless – CCNA Wireless, 2013
- Cisco Certified Network Associate Security – CCNA Security, 2013
- VMware Certified Professional 6 – Data Center Virtualization – VCP6-DCV, 2016

James Chacko – Cyber Security SME

James is a senior cyber security professional with over 20 years of progressive experience, specializing in critical infrastructure projects across utilities, water and wastewater, transit, oil and gas, hospitality, and retail industries. With a diverse and extensive skill set, James specializes in developing robust cyber security programs and conducting detailed security assessments. This expertise is complemented by his proficiency in Operations and Technical Support, Systems/Network Administration, Business Technical Analysis, and Project Management. Proficient in

identifying and mitigating vulnerabilities across IT/OT infrastructure, James is adept at developing and

implementing policies and procedures to bolster resiliency. His ability to effectively bridge communication between executive management, vendors, technical teams, and end-users enhances his project leadership capabilities. Demonstrating strong competence in managing budgets and resources and armed with robust communication and reporting skills, James is deeply committed to continuous learning and professional development. James is advancing his knowledge in the field by pursuing a Master of Science degree in Cybersecurity (Cyber-Physical Systems) at the Georgia Institute of Technology, Atlanta, GA.

Relevant Experience:

- Conducted a comprehensive security audit of a key vendor's Development and Build environments, manufacturing processes, and the product, assessing compliance with NIST standards for Advanced Metering Infrastructure (AMI) 2.0, which led to significant enhancements in their security postures
- Led a comprehensive cyber fraud review for a corporate group finance, assessing transactional processes and PII handling, and provided actionable recommendations to enhance security and prevent fraudulent activities
- Developed and implemented multiple patch management programs for various utilities across North America, enhancing their cyber security posture
- Supported the creation and ongoing revision of security architecture and policy & procedures documentation, adhering to standards like the NIST Cyber Security Framework, NERC CIP standards, and the Ontario Cyber Security Framework
- Conducted extensive web application tests, vulnerability assessments, and penetration tests for clients such as NB Power, ATCO, EPCOR, Utilities Standard Forum (USF), Crosslinx Transit Operators, Missouri Public Utility Alliance, and Georgia Systems Operations Centre
- Provided detailed remediation guidance post-audits and assessments to secure client systems and infrastructure
- Played a crucial role in black box-type penetration testing against critical devices in smart grid networks, evaluating device security and contributing to the network's overall safety
- Conducted wireless assessments at various client sites, ensuring the implementation of best practices and identifying potential vulnerabilities
- Streamlined the process for identifying and categorizing BES Cyber Systems and associated assets based on NERC CIP standards
- Documented enabled listening ports on BES Cyber Assets in OT environments, providing operational justification for ATCO Electric as per NERC CIP standards
- Assisted in remediating findings from NERC CIP audits for generation and distribution utilities
- Served as an expert security analyst for closed-loop monitoring services, overseeing SOC activities, including network-level monitoring and log analysis, and providing expert remediation guidance
- Collaborated with organizations in investigating security incidents, determining origins and methods of attack, and formulating prevention strategies for future threats

- Researched threat advisories and security breaches, guiding utilities to address concerns and secure their systems
- Engaged in research on next-generation cyber security tools, software applications, and solutions
- Developed and delivered IT/OT cyber security training programs across North America for the utility sector
- Contributed to developing an American Public Power Association (APPA) survey, focusing on data collection and evaluation of "data-in-motion"
- Completed a business analysis for IT-OT convergence, aligning organizational strategies and technologies
- Led the implementation of OSIsoft's PI System, including configuration, user permissions, and system integration, to optimize asset management and data analysis capabilities

License, Certifications and Contact Information:

- Contact: **E:** jamesc@aesi-inc.com **P:** 770.870.1630 x. 261
- Master of Science – Cybersecurity (Cyber-physical Systems), Georgia Institute of Technology, USA, in progress
- Master of International Business, University of Wollongong, Australia, 2007
- Bachelor of Technology – Information Technology, University of Madras, India

Alex Lian – Cyber Security SME

Alex is a highly skilled software development and network professional with experience in cyber security assessments, E-Learning and digital media, and web and application development. He has experience in vulnerability analysis and research and has conducted cyber security assessments for various North American utilities. Alex holds an Advanced Diploma in Software Development and Network Engineering from Sheridan College and a Bachelor of Engineering in Aerospace Engineering from Ryerson University, which provides a unique approach to problem analysis and solution implementation. He is adept at collaborating with cross-functional teams and delivering high-quality training programs and web applications, possesses strong communication and teamwork skills, pays close attention to detail, and is skilled in troubleshooti ng and technical problem-solving.

Relevant Experience:

- Conducted a comprehensive security audit of a key vendor's Development and Build environments, manufacturing processes, and the product, assessing compliance with NIST standards for Advanced Metering Infrastructure
- Conducted patch assessment programs for various North American utilities
- Conducted research on various utility programs in terms of cyber security

- Converted cyber security standards from one jurisdiction to another, based on company assets,

requirements, and location

- Tested basic penetration testing and vulnerability assessment commands/scripts using Kali Linux
- Evaluated and expanded upon outputs from Nessus vulnerability assessments to provide accurate and actionable Conducted NERC CIP and O&P mock audits for all registered entities types

License, Certifications and Contact Information:

- Contact: **E:** alexl@aesi-inc.com , **P:** 770.870.1630 x. 279
- Advanced Diploma, Software Development and Network Engineering, Sheridan College
- Bachelor of Engineering, Aerospace Engineering, Ryerson University

Nathan Chang – Cyber Security SME

Nathan is a skilled developer and security analyst with experience in cyber security analysis, vulnerability management, and process automation. He has conducted cyber operations for North American utilities regarding vulnerability analysis, assessing patches, advising remediation plans based on security priorities, and creating detailed reports based on current cyber threats. Nathan possesses an Advanced Diploma in Software Development and Network Engineering from Sheridan College, equipping him with a distinctive method for analysing problems and executing solutions. Capable of collaborating with multiple cross-functional teams, he excels in delivering high-quality security reports and automated solutions. He possesses strong communication and teamwork skills, pays close attention to detail, and is skilled in troubleshooting and technical problem-solving.

Relevant Experience:

- Led detailed social engineering campaigns, leveraging advanced web design concepts to formulate believable phishing emails to test organizations' security posture, and offer actionable Cyber Security enhancement strategies to compromised users
- Designed and implemented automated solutions to enhance Patch Assessment and Cyber Vulnerability Analysis procedures, leveraging the Microsoft security API and scalable database interfaces to increase efficiency and precision in vulnerability mitigation
- Aided in deploying real-time vulnerability management solutions enabling security operations members to monitor their assets and vulnerabilities in real time, while facilitating security exception requests, managing their vulnerabilities through the MS Azure DevOps platform, improving remediation and vulnerability ownership

- Conducted Patch Assessment Programs across North American utilities in compliance with NERC CIP guidelines, enhancing cyber security measures through the identification and resolution of security vulnerabilities enforcing NERC CIP -007 standards.
- Experienced with configuring various intrusion detection and SIEM systems to gather network traffic, pinpoint potential security threats, and take swift action to minimize risks enforcing NERC CIP-007 standards.
- Immersed in research and analysis of advanced security solutions, encompassing intrusion methods and the required toolset for prevention, tailoring Cyber Security strategies to suit a variety of jurisdictions for a holistic approach to asset protection.

License, Certifications and Contact Information:

- Contact: **E:** nathanc@aesi-inc.com , **P:** 770.870.1630 x. 280

- Advanced Diploma, Software Development and Network Engineering, Sheridan College