

TXShare

Your Public Sector Solutions Center

MASTER SERVICES AGREEMENT #2025-018 Artificial Intelligence (AI) Solutions for Public Sector Entities

THIS MASTER SERVICES AGREEMENT ("Agreement"), effective the last date of signed approval ("Effective Date"), is entered into by and between the **North Central Texas Council of Governments** ("**NCTCOG**"), a Texas political subdivision and non-profit corporation, with offices located at 616 Six Flags Drive, Arlington, TX 76011, and

V3Main Technologies, Inc. ("Contractor")
3215 Brinmont Place LN
Katy, TX 77494

ARTICLE I RETENTION OF THE CONTRACTOR

1.1 This Agreement defines the terms and conditions upon which the Contractor agrees to provide **Artificial Intelligence (AI) Solutions for Public Sector Entities** (hereinafter, "Services") to governmental entities participating in the TXShare program (hereinafter "Participating Entities"). The Contractor is being retained to provide services described below to Participating Entities based on the Contractor's demonstrated competence and requisite qualifications to perform the scope of the services described herein and in the Request for Proposals #2025-018 (hereinafter, "RFP"). The Contractor demonstrated they have the resources, experience, and qualifications to perform the described services, which is of interest to Participating Entities and was procured via the RFP. NCTCOG agrees to and hereby does retain the Contractor, as an independent contractor, and the Contractor agrees to provide services to Participating Entities, in accordance with the terms and conditions provided in this Agreement and consistent with Contractor's response to the RFP.

ARTICLE II SCOPE OF SERVICES

- 2.1 The Contractor will provide Services described in a written Purchase Order issued by NCTCOG or a SHARE Participating Entity. Any such Purchase Order is hereby incorporated by reference and made a part of this Agreement and shall be subject to the terms and conditions in this Agreement. In the event of a conflict between any term or provision in this Agreement and any term or provision in a Purchase Order, the term or provision in this Agreement shall control unless the conflicting term or provision in this Agreement is referenced, and expressly stated not to apply, in such Purchase Order.
- 2.2 All Services rendered under this Agreement will be performed by the Contractor: i) with due care; ii) in accordance with generally prevailing industry standards; iii) in accordance with Participating Entities' standard operating procedures and applicable policies, as may be amended from time to time; and iv) in compliance with all applicable laws, government regulatory requirements, and any other written instructions, specifications, guidelines, or requirements provided by NCTCOG and/or Participating Entities.
- 2.3 Any agreed-upon changes to a Purchase Order shall be set forth in a subsequent Purchase Order amendment. Contractor will not implement any changes or any new Services until a Purchase Order has been duly executed by Participating Entity. For the avoidance of doubt, the Contractor acknowledges that Participating Entity is under no obligation to execute a Purchase Order. Participating

Entity shall not be liable for any amounts not included in a Purchase Order in the absence of a fully executed amendment of Purchase Order.

- 2.4 Percentage discounts for items in Appendix A represent the minimum discounts provided for each item within the category offered by the Contractor. Contractor and Participating Entity may mutually agree to a greater percentage discount for any item covered under this agreement.

2.5 NCTCOG Obligations

- 2.5.1 NCTCOG shall make available a contract page on its TXShare.org website which will include contact information for the Contractor(s).

2.6 Participating Entity Obligations.

- 2.6.1 In order to utilize the Services, Participating Entities must have executed a Master Interlocal Agreement for TXShare with NCTCOG. This agreement with the Participating Entity will define the legal relationship between NCTCOG and the Participating Entity.
- 2.6.2 In order to utilize the Services, Participating Entities must execute a Purchase Order with the Contractor. This agreement with the Participating Entity will define the Services and costs that the Participating Entity desires to have implemented by the Contractor.

2.7 Contractor Obligations.

- 2.7.1 Contractor must be able to deliver, perform, install, and implement services with the requirements and intent of RFP #2025-018.
- 2.7.2 If applicable, Contractor shall provide all necessary material, labor and management required to perform this work. The scope of services shall include, but not be limited to, items listed in Appendix A.
- 2.7.3 Contractor agrees to market and promote the use of the SHARE awarded contract whenever possible among its current and solicited customer base. Contractor shall agree to follow reporting requirements in report sales made under this Master Services Agreement in accordance with Section 4.2.

ARTICLE III

TERM

- 3.1 This Agreement will commence on the Effective Date and remain in effect for an initial term ending on May 31, 2027 (the “**Term**”), unless earlier terminated as provided herein. This Agreement will automatically be renewed, unless NCTCOG explicitly desires otherwise, for up to three (3) additional one (1) year terms through May 31, 2030.
- 3.2 **Termination.** NCTCOG and/or Participating Entities may terminate this Agreement and/or any Purchase Order to which it is a signatory at any time, with or without cause, upon thirty (30) days’ prior written notice to Contractor. Upon its receipt of notice of termination of this Agreement or Purchase Order, Contractor shall follow any instructions of NCTCOG respecting work stoppage. Contractor shall cooperate with NCTCOG and/or Participating Entities to provide for an orderly conclusion of the Services. Contractor shall use its best efforts to minimize the amount of any non-cancelable obligations and shall assign any contracts related thereto to NCTCOG or Participating Entity at its request. If NCTCOG or Participating Entity elects to continue any activities underlying a terminated Purchase Order after termination, Contractor shall cooperate with NCTCOG or Participating Entity to provide for an orderly transfer of Contractor’s responsibilities with respect to such Purchase Order to NCTCOG or Participating Entity. Upon the effective date of any such termination, the Contractor shall submit a final invoice for payment in accordance with Article IV, and NCTCOG or Participating Entity shall pay such amounts as are due to Contractor through the effective date of termination. NCTCOG or Participating Entity shall only be liable for payment of services rendered before the effective date of termination. If Agreement is terminated, certain reporting requirements identified in this Agreement shall survive termination of this Agreement.

- 3.2.1 Termination for Convenience: Either party may terminate the agreement for its convenience in whole or in part at any time without cause, upon 30 days written notice. Upon termination for convenience, the contractor will be entitled to payment for goods or services satisfactorily performed or delivered.
- 3.2.2 Termination for Cause: Either party may immediately terminate this Agreement if the other party breaches its obligations specified within this Agreement, and, where capable of remedy, such breach has not been materially cured within thirty (30) days of the breaching party's receipt of written notice describing the breach in reasonable detail.
- 3.2.3 Termination for Breach: Upon any material breach of this Agreement by either party, the non-breaching party may terminate this Agreement upon twenty (20) days written notice to the breaching party. The notice shall become effective at the end of the twenty (20) day period unless the breaching party cures such breach within such period.

ARTICLE IV COMPENSATION

- 4.1 **Invoices.** Contractor shall submit an invoice to the ordering Participating Entity upon receipt of an executed Purchase Order and after completion of the work, with Net 30 payment terms. Costs incurred prior to execution of this Agreement are not eligible for reimbursement. There shall be no obligation whatsoever to pay for performance of this Agreement from the monies of the NCTCOG or Participating Entities, other than from the monies designated for this Agreement and/or executed Purchase Order. Contractor expressly agrees that NCTCOG shall not be liable, financial or otherwise, for Services provided to Participating Entities.
- 4.2 **Reporting.** NCTCOG intends to make this Agreement available to other governmental entities through its TXShare cooperative purchasing program. NCTCOG has contracted Civic Marketplace as a digital marketplace for selected TXShare awarded contracts and to serve as NCTCOG's collector of reports and remunerative fees referenced in Section 5.2 of the Master Services Agreement. Unless otherwise directed in writing by NCTCOG, Contractor shall submit to Civic Marketplace on a calendar quarterly basis a report that identifies any new client Participating Entities, the date(s) and order number(s), and the total contracted value of service(s) that each Participating Entity has purchased and paid in full under this Master Service Agreement. Reporting and invoices should be submitted to:

Civic Marketplace, Inc.
6502 Glen Abbey
Abilene, TX 79606
Email: support@civicmarketplace.com

ARTICLE V SERVICE FEE

- 5.1 **Explanation.** NCTCOG will make this Master Service Agreement available to other governmental entities, Participating Entities, and non-profit agencies in Texas and the rest of the United States through its SHARE cooperative purchasing program. The Contractor is able to market the Services under this Agreement to any Participating Entity with emphasis that competitive solicitation is not required when the Participating Entity purchases off of a cooperative purchasing program such as SHARE. However, each Participating Entity will make the decision that it feels is in compliance with its own purchasing requirements. The Contractor realizes substantial efficiencies through their ability to offer pricing through the SHARE Cooperative and that will increase the sales opportunities as well as reduce the need to repeatedly respond to Participating Entities' Requests for Proposals. From these efficiencies, Contractor will pay an administrative fee to SHARE calculated as a percentage of sales processed through the SHARE Master Services Agreement. This administrative fee is not an added cost to SHARE participants. This administrative fee covers the costs of solicitation of the contract, marketing and facilitation, as well as offsets expenses incurred by SHARE.

5.2 **Administrative Fee.** NCTCOG will utilize an administrative fee, in the form of a percent of cost that will apply to all contracts between awarded contractor and NCTCOG or participants resulting from this solicitation. The administrative fee will be remitted by the contractor to Civic Marketplace on a quarterly basis, along with required quarterly reporting. The remuneration fee for this program will be 2.5% on sales.

5.3 **Setup and Implementation.** NCTCOG will provide instruction and guidance as needed to the Contractor to assist in maximizing mutual benefits from marketing these Services through the SHARE purchasing program.

ARTICLE VI RELATIONSHIP BETWEEN THE PARTIES

6.1 **Contractual Relationship.** It is understood and agreed that the relationship described in this Agreement between the Parties is contractual in nature and is not to be construed to create a partnership or joint venture or agency relationship between the parties. Neither party shall have the right to act on behalf of the other except as expressly set forth in this Agreement. Contractor will be solely responsible for and will pay all taxes related to the receipt of payments hereunder and shall give reasonable proof and supporting documents, if reasonably requested, to verify the payment of such taxes. No Contractor personnel shall obtain the status of or otherwise be considered an employee of NCTCOG or Participating Entity by virtue of their activities under this Agreement.

ARTICLE VII REPRESENTATION AND WARRANTIES

7.1 **Representations and Warranties.** Contractor represents and warrants that:

- 7.1.1 As of the Effective Date of this Agreement, it is not a party to any oral or written contract or understanding with any third party that is inconsistent with this Agreement and/or would affect the Contractor's performance under this Agreement; or that will in any way limit or conflict with its ability to fulfill the terms of this Agreement. The Contractor further represents that it will not enter into any such agreement during the Term of this Agreement;
- 7.1.2 NCTCOG is prohibited from making any award or permitting any award at any tier to any party which is debarred or suspended or otherwise excluded from, or ineligible for, participation in federal assistance programs under Executive Order 12549, Debarment and Suspension. Contractor and its subcontractors shall include a statement of compliance with Federal and State Debarment and suspension regulations in all Third-party contracts.
- 7.1.3 Contractor shall notify NCTCOG if Contractor or any of the Contractor's sub-contractors becomes debarred or suspended during the performance of this Agreement. Debarment or suspension of the Contractor or any of Contractor's sub-contractors may result in immediate termination of this Agreement.
- 7.1.4 Contractor and its employees and sub-contractors have all necessary qualifications, licenses, permits, and/or registrations to perform the Services in accordance with the terms and conditions of this Agreement, and at all times during the Term, all such qualifications, licenses, permits, and/or registrations shall be current and in good standing.
- 7.1.5 Contractor shall, and shall cause its representatives to, comply with all municipal, state, and federal laws, rules, and regulations applicable to the performance of the Contractor's obligations under this Agreement.

ARTICLE VIII CONFIDENTIAL INFORMATION AND OWNERSHIP

- 8.1 **Confidential Information.** Contractor acknowledges that any information it or its employees, agents, or subcontractors obtain regarding the operation of NCTCOG or Participating Entities, its products, services, policies, customer, personnel, and other aspect of its operation (“Confidential Information”) is proprietary and confidential, and shall not be revealed, sold, exchanged, traded, or disclosed to any person, company, or other entity during the period of the Contractor’s retention hereunder or at any time thereafter without the express written permission of NCTCOG or Participating Entity.

Notwithstanding anything in this Agreement to the contrary, Contractor shall have no obligation of confidentiality with respect to information that (i) is or becomes part of the public domain through no act or omission of Contractor; (ii) was in Contractor’s lawful possession prior to the disclosure and had not been obtained by Contractor either directly or indirectly from the NCTCOG or Participating Entity; (iii) is lawfully disclosed to Contractor by a third party without restriction on disclosure; (iv) is independently developed by Contractor without use of or reference to the NCTCOG’s Participating Entity’s Confidential Information; or (v) is required to be disclosed by law or judicial, arbitral or governmental order or process, provided Contractor gives the NCTCOG or Participating Entity prompt written notice of such requirement to permit the NCTCOG or Participating Entity to seek a protective order or other appropriate relief. Contractor acknowledges that NCTCOG and Participating Entities must strictly comply with applicable public information laws, in responding to any request for public information. This obligation supersedes any conflicting provisions of this Agreement.

- 8.2 **Ownership.** No title or ownership rights to any applicable software are transferred to the NCTCOG by this agreement. The Contractor and its suppliers retain all right, title and interest, including all copyright and intellectual property rights, in and to, the software (as an independent work and as an underlying work serving as a basis for any improvements, modifications, derivative works, and applications NCTCOG may develop), and all copies thereof. All final documents, data, reports, information, or materials are and shall at all times be and remain, upon payment of Contractor’s invoices therefore, the property of NCTCOG or Participating Entity and shall not be subject to any restriction or limitation on their future use by, or on behalf of, NCTCOG or Participating Entity, except otherwise provided herein. Subject to the foregoing exception, if at any time demand be made by NCTCOG or Participating Entity for any documentation related to this Agreement and/or applicable Purchase Orders for the NCTCOG and/or any Participating Entity, whether after termination of this Agreement or otherwise, the same shall be turned over to NCTCOG without delay, and in no event later than thirty (30) days after such demand is made. Contractor shall have the right to retain copies of documentation, and other items for its archives. If for any reason the foregoing Agreement regarding the ownership of documentation is determined to be unenforceable, either in whole or in part, the Contractor hereby assigns and agrees to assign to NCTCOG all rights, title, and interest that the Contractor may have or at any time acquire in said documentation and other materials, provided that the Contractor has been paid the aforesaid.

ARTICLE IX GENERAL PROVISIONS

- 9.1 **Notices.** All notices from one Party to another Party regarding this Agreement shall be in writing and delivered to the addresses shown below:

If to NCTCOG:	North Central Texas Council of Governments P.O. Box 5888 Arlington, TX 76005-5888 Attn: Purchasing Agent Phone Number: 817-704-5674 elittrell@nctcog.org
---------------	---

If to Contractor:

V3Main Technologies, Inc.

Attn: Venkat Maddikayala

3215 Brinmont Place LN

Katy, TX 77494

Phone: 281-769-3935

Email: Venkat.maddikayala@v3main.com

The above contact information may be modified without requiring an amendment to the Agreement.

9.2 **Tax.** NCTCOG and several participating entities are exempt from Texas limited sales, federal excise and use tax, and does not pay tax on purchase, rental, or lease of tangible personal property for the organization's use. A tax exemption certificate will be issued upon request.

9.3 **Indemnification.** Contractor shall defend, indemnify, and hold harmless NCTCOG and Participating Entities, NCTCOG's affiliates, and any of their respective directors, officers, employees, agents, subcontractors, successors, and assigns from any and all suits, actions, claims, demands, judgments, liabilities, losses, damages, costs, and expenses (including reasonable attorneys' fees and court costs) (collectively, "Losses") arising out of or relating to: (i) Services performed and carried out pursuant to this Agreement; (ii) breach of any obligation, warranty, or representation in this Agreement, (iii) the negligence or willful misconduct of Contractor and/or its employees or subcontractors; or (iv) any infringement, misappropriation, or violation by Contractor and/or its employees or subcontractors of any right of a third party; provided, however, that Contractor shall have no obligation to defend, indemnify, or hold harmless to the extent any Losses are the result of NCTCOG's or Participating Entities' gross negligence or willful misconduct.

9.4 **Limitation of Liability.** In no event shall either party be liable for special, consequential, incidental, indirect or punitive loss, damages or expenses arising out of or relating to this Agreement, whether arising from a breach of contract or warranty, or arising in tort, strict liability, by statute or otherwise, even if it has been advised of their possible existence or if such loss, damages or expenses were reasonably foreseeable.

Notwithstanding any provision hereof to the contrary, neither party's liability shall be limited by this Article with respect to claims arising from breach of any confidentiality obligation, arising from such party's infringement of the other party's intellectual property rights, covered by any express indemnity obligation of such party hereunder, arising from or with respect to injuries to persons or damages to tangible property, or arising out of the gross negligence or willful misconduct of the party or its employees.

9.5 **Insurance.** At all times during the term of this Agreement, Contractor shall procure, pay for, and maintain, with approved insurance carriers, the minimum insurance requirements set forth below, unless otherwise agreed in a Purchase Order between Contractor and Participating Entities. Further, Contractor shall require all contractors and sub-contractors performing work for which the same liabilities may apply under this Agreement to do likewise. All subcontractors performing work for which the same liabilities may apply under this contract shall be required to do likewise. Contractor may cause the insurance to be effected in whole or in part by the contractors or sub-contractors under their contracts. NCTCOG reserves the right to waive or modify insurance requirements at its sole discretion.

9.5.1 Workers' Compensation: Statutory limits and employer's liability of \$100,000 for each accident or disease.

9.5.2 Commercial General Liability:

9.5.2.1 Required Limits:

\$1,000,000 per occurrence;

\$3,000,000 Annual Aggregate

9.5.2.2 Commercial General Liability policy shall include:

9.5.2.2.1 Coverage A: Bodily injury and property damage;

- 9.5.2.2.2 Coverage B: Personal and Advertising Injury liability;
 - 9.5.2.2.3 Coverage C: Medical Payments;
 - 9.5.2.2.4 Products: Completed Operations;
 - 9.5.2.2.5 Fire Legal Liability;
 - 9.5.2.3 Policy coverage must be on an “occurrence” basis using CGL forms as approved by the Texas State Board of Insurance.
- 9.5.3 Business Auto Liability: Coverage shall be provided for all owned hired, and non-owned vehicles. Required Limit: \$1,000,000 combined single limit each accident.
- 9.5.4 Professional Errors and Omissions liability:
 - 9.5.4.1 Required Limits:
 - \$1,000,000 Each Claim
 - \$1,000,000 Annual Aggregate
- 9.6 **Conflict of Interest.** During the term of this Agreement, and all extensions hereto and for a period of one (1) year thereafter, neither party, shall, without the prior written consent of the other, directly or indirectly, whether for its own account or with any other persons or entity whatsoever, employ, solicit to employ or endeavor to entice away any person who is employed by the other party.
- 9.7 **Force Majeure.** It is expressly understood and agreed by both parties to this Agreement that, if the performance of any provision of this Agreement is delayed by force majeure, defined as reason of war, civil commotion, act of God, governmental restriction, regulation or interference, fire, explosion, hurricane, flood, failure of transportation, court injunction, or any circumstances which are reasonably beyond the control of the party obligated or permitted under the terms of this Agreement to do or perform the same, regardless of whether any such circumstance is similar to any of those enumerated herein, the party so obligated or permitted shall be excused from doing or performing the same during such period of delay, so that the period of time applicable to such requirement shall be extended for a period of time equal to the period of time such party was delayed. Each party must inform the other in writing within a reasonable time of the existence of such force majeure.
- 9.8 **Ability to Perform.** Contractor agrees promptly to inform NCTCOG of any event or change in circumstances which may reasonably be expected to negatively affect the Contractor’s ability to perform its obligations under this Agreement in the manner contemplated by the parties.
- 9.9 **Availability of Funding.** This Agreement and all claims, suits, or obligations arising under or related to this Agreement are subject to and limited by the receipt and availability of funds which are received from the Participating Entities by NCTCOG dedicated for the purposes of this Agreement.
- 9.10 **Governing Law.** This Agreement will be governed by and construed in accordance with the laws of the State of Texas, United States of America. The mandatory and exclusive venue for the adjudication or resolution of any dispute arising out of this Agreement shall be in Tarrant County, Texas.
- 9.11 **Waiver.** Failure by either party to insist on strict adherence to any one or more of the terms or conditions of this Agreement, or on one or more occasions, will not be construed as a waiver, nor deprive that party of the right to require strict compliance with the same thereafter.
- 9.12 **Entire Agreement.** This Agreement and any attachments/addendums, as provided herein, constitutes the entire agreement of the parties and supersedes all other agreements, discussions, representations or understandings between the parties with respect to the subject matter hereof. No amendments hereto, or waivers or releases of obligations hereunder, shall be effective unless agreed to in writing by the parties hereto.

- 9.13 **Assignment.** This Agreement may not be assigned by either Party without the prior written consent of the other Party.
- 9.14 **Severability.** In the event any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision(s) hereof, and this Agreement shall be revised so as to cure such invalid, illegal, or unenforceable provision(s) to carry out as near as possible the original intents of the Parties.
- 9.15 **Amendments.** This Agreement may be amended only by a written amendment executed by both Parties, except that any alterations, additions, or deletions to the terms of this Agreement, which are required by changes in Federal and State law or regulations or required by the funding source, are automatically incorporated into this Agreement without written amendment hereto and shall become effective on the date designated by such law or regulation.
- 9.16 **Dispute Resolution.** The parties to this Agreement agree to the extent possible and not in contravention of any applicable State or Federal law or procedure established for dispute resolution, to attempt to resolve any dispute between them regarding this Agreement informally through voluntary mediation, arbitration or any other local dispute mediation process, including but not limited to dispute resolution policies of NCTCOG, before resorting to litigation.
- 9.17 **Publicity.** Contractor shall not issue any press release or make any statement to the media with respect to this Agreement or the services provided hereunder without the prior written consent of NCTCOG.
- 9.18 **Survival.** Rights and obligations under this Agreement which by their nature should survive will remain in effect after termination or expiration hereof.

ARTICLE X ADDITIONAL REQUIREMENTS

- 10.1 **Equal Employment Opportunity.** Contractor shall not discriminate against any employee or applicant for employment because of race, religion, color, sex, sexual orientation, gender identity, or national origin. Contractor shall take affirmative actions to ensure that applicants are employed, and that employees are treated, during their employment, without regard to their race, religion, color, sex, sexual orientation, gender identity, or national origin. Such actions shall include, but not be limited to, the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.
- 10.2 **Davis-Bacon Act.** Contractor agrees to comply with all applicable provisions of 40 USC § 3141 – 3148.
- 10.3 **Contract Work Hours and Selection Standards.** Contractor agrees to comply with all applicable provisions of 40 USC § 3701 – 3708 to the extent this Agreement indicates any employment of mechanics or laborers.
- 10.4 **Rights to Invention Made Under Contract or Agreement.** Contractor agrees to comply with all applicable provisions of 37 CFR Part 401.
- 10.5 **Clean Air Act, Federal Water Pollution Control Act, and Energy Policy Conservation Act.** Contractor agrees to comply with all applicable provisions of the Clean Air Act under 42 USC § 7401 – 7671, the Energy Federal Water Pollution Control Act 33 USC § 1251 – 1387, and the Energy Policy Conservation Act under 42 USC § 6201.
- 10.6 **Debarment/Suspension.** Contractor is prohibited from making any award or permitting any award at any tier to any party which is debarred or suspended or otherwise excluded from or ineligible for

participation in federal assistance programs under Executive Order 12549, Debarment and Suspension. Contractor and its subcontractors shall comply with the Certification Requirements for Recipients of Grants and Cooperative Agreements Regarding Debarments and Suspensions.

- 10.7 **Restrictions on Lobbying.** CONTRACTOR agrees to comply with all applicable provisions of 2 CFR §200.450. CONTRACTOR shall include a statement of compliance with the Lobbying Certification and Disclosure of Lobbying Activities in procurement solicitations exceeding \$100,000. Lobbying Certification and Disclosure of Lobbying Activities shall be completed by subcontractors and included in subcontractor contracts, as applicable. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. See Appendix C.
- 10.8 **Procurement of Recovered Materials.** Contractor agrees to comply with all applicable provisions of 2 CFR §200.322.
- 10.9 **Drug-Free Workplace.** Contractor shall provide a drug free work place in compliance with the Drug Free Work Place Act of 1988.
- 10.10 **Texas Corporate Franchise Tax Certification.** Pursuant to Article 2.45, Texas Business Corporation Act, state agencies may not contract with for profit corporations that are delinquent in making state franchise tax payments.

10.11 **Civil Rights Compliance**

Compliance with Regulations: Contractor will comply with the Acts and the Regulations relative to Nondiscrimination in Federally-assisted programs of the U.S. Department of Transportation (USDOT), the Federal Highway Administration (FHWA), as they may be amended from time to time, which are herein incorporated by reference and made part of this agreement.

Nondiscrimination: Contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, sex, or national origin in the selection and retention of subcontractors, including procurement of materials and leases of equipment. Contractor will not participate directly or indirectly in the discrimination prohibited by the Acts and the Regulations, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 45 CFR Part 21.

Solicitations for Subcontracts, Including Procurement of Materials and Equipment: In all solicitations either by competitive bidding or negotiation made by Contractor for work to be performed under a subcontract, including procurement of materials or leases of equipment, each potential subcontractor or supplier will be notified by Contractor of obligations under this contract and the Acts and Regulations relative to Nondiscrimination on the grounds of race, color, sex, or national origin.

Information and Reports: Contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto, and will permit access to its books, records, accounts, other sources of information, and facilities as may be determined by the State or the FHWA to be pertinent to ascertain compliance with such Acts, Regulations or directives. Where any information required of Contractor is in the exclusive possession of another who fails or refuses to furnish this information, Contractor will so certify to NCTCOG, the Texas Department of Transportation (“the State”) or the Federal Highway Administration, as appropriate, and will set forth what efforts it has made to obtain the information.

Sanctions for Noncompliance: In the event of Contractor's noncompliance with the Nondiscrimination provisions of this Agreement, NCTCOG will impose such sanctions as it or the State or the FHWA may determine to be appropriate, including, but not limited to: withholding of payments to the Contractor under this Agreement until the Contractor compiles and/or cancelling, terminating or suspension of this Agreement, in whole or in part.

Incorporation of Provisions: Contractor will include the provisions of the paragraphs listed above, in this section 10.11, in every subcontract, including procurement of materials and leases of equipment, unless exempt by the Acts, the Regulations and directives issued pursuant thereto. Contractor will take such action with respect to any subcontract or procurement as NCTCOG, the State, or the FHWA may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if Contractor becomes involved in, or is threatened with, litigation with a subcontractor or supplier because of such direction, Contractor may request the State to enter into such litigation to protect the interests of the State. In addition, Contractor may request the United States to enter into such litigation to protect the interests of the United States.

10.12 **Disadvantaged Business Enterprise Program Requirements**

Contractor shall not discriminate on the basis of race, color, national origin, or sex in the award and performance of any U.S. Department of Transportation (DOT)-assisted contract or in the administration of its DBE program or the requirements of 49 CFR Part 26. Contractor shall take all necessary and reasonable steps under 49 CFR Part 26 to ensure non-discrimination in award and administration of DOT-assisted contracts. Each sub-award or sub-contract must include the following assurance: *The Contractor, sub-recipient, or sub-contractor shall not discriminate on the basis of race, color, national origin, or sex in the performance of this Agreement. The Contractor shall carry out applicable requirements of 49 CFR Part 26 in the award and administration of DOT-assisted contracts. Failure by the Contractor to carry out these requirements is a material breach of this agreement, which may result in the termination of this agreement or such other remedy as the recipient deems appropriate.*

10.13 **Pertinent Non-Discrimination Authorities**

During the performance of this Agreement, Contractor, for itself, its assignees, and successors in interest agree to comply with the following nondiscrimination statutes and authorities; including but not limited to:

- a. Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d et seq., 78 stat. 252), (prohibits discrimination on the basis of race, color, national origin); and 49 CFR Part 21.
- b. The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 U.S.C. § 4601), (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects).
- c. Federal-Aid Highway Act of 1973, (23 U.S.C. § 324 et seq.), as amended, (prohibits discrimination on the basis of sex).
- d. Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. § 794 et seq.) as amended, (prohibits discrimination on the basis of disability); and 49 CFR Part 27.
- e. The Age Discrimination Act of 1975, as amended, (49 U.S.C. § 6101 et seq.), (prohibits discrimination on the basis of age).
- f. Airport and Airway Improvement Act of 1982, (49 U.S.C. Chapter 471, Section 47123), as amended, (prohibits discrimination based on race, creed, color, national origin, or sex).
- g. The Civil Rights Restoration Act of 1987, (PL 100-209), (Broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, The Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, subrecipients and contractors, whether such programs or activities are Federally funded or not).
- h. Titles II and III of the Americans with Disabilities Act, which prohibits discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities (42 U.S.C. §§ 12131-12189) as implemented by Department of Transportation regulations at 49 C.F.R. parts 37 and 38.

- i. The Federal Aviation Administration’s Nondiscrimination statute (49 U.S.C. § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex).
- j. Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which ensures nondiscrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations.
- k. Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, the parties must take reasonable steps to ensure that LEP persons have meaningful access to the programs (70 Fed. Reg. at 74087 to 74100).
- i. Title IX of the Education Amendments of 1972, as amended, which prohibits the parties from discriminating because of sex in education programs or activities (20 U.S.C. 1681 et seq.).

10.14 Ineligibility to Receive State Grants or Loans, or Receive Payment on State Contracts

In accordance with Section 231.006 of the Texas Family Code, a child support obligor who is more than thirty (30) days delinquent in paying child support and a business entity in which the obligor is a sole proprietor, partner, shareholder, or owner with an ownership interest of at least twenty-five (25) percent is not eligible to:

- a. Receive payments from state funds under a contract to provide property, materials or services; or
- b. Receive a state-funded grant or loan.

By signing this Agreement, the Contractor certifies compliance with this provision.

10.15 House Bill 89 Certification

If contractor is required to make a certification pursuant to Section 2270.002 of the Texas Government Code, contractor certifies that contractor does not boycott Israel and will not boycott Israel during the term of the contract resulting from this solicitation. If contractor does not make that certification, contractor state in the space below why the certification is not required.

10.16 Certification Regarding Disclosure of Conflict of Interest.

The undersigned certifies that, to the best of his or her knowledge or belief, that:

“No employee of the contractor, no member of the contractor’s governing board or body, and no person who exercises any functions or responsibilities in the review or approval of the undertaking or carrying out of this contract shall participate in any decision relating to this contract which affects his/her personal pecuniary interest.

Executives and employees of contractor shall be particularly aware of the varying degrees of influence that can be exerted by personal friends and associates and, in administering the contract, shall exercise due diligence to avoid situations which give rise to an assertion that favorable treatment is being granted to friends and associates. When it is in the public interest for the contractor to conduct business with a friend or associate of an executive or employee of the contractor, an elected official in the area or a member of the North Central Texas Council of Governments, a permanent record of the transaction shall be retained.

Any executive or employee of the contractor, an elected official in the area or a member of the NCTCOG, shall not solicit or accept money or any other consideration from a third person, for the performance of an act reimbursed in whole or part by contractor or Department. Supplies, tools, materials, equipment or services purchased with contract funds shall be used solely for purposes allowed under this contract. No member of the NCTCOG shall cast a vote on the provision of services by that member (or any organization which that member represents) or vote on any matter

which would provide a direct or indirect financial benefit to the member or any business or organization which the member directly represents.”

No officer, employee or paid consultant of the contractor is a member of the NCTCOG.

No officer, manager or paid consultant of the contractor is married to a member of the NCTCOG.

No member of NCTCOG directly owns, controls or has interest in the contractor.

The contractor has disclosed any interest, fact, or circumstance that does or may present a potential conflict of interest.

No member of the NCTCOG receives compensation from the contractor for lobbying activities as defined in Chapter 305 of the Texas Government Code.

Should the contractor fail to abide by the foregoing covenants and affirmations regarding conflict of interest, the contractor shall not be entitled to the recovery of any costs or expenses incurred in relation to the contract and shall immediately refund to the North Central Texas Council of Governments any fees or expenses that may have been paid under this contract and shall further be liable for any other costs incurred or damages sustained by the NCTCOG as it relates to this contract.

10.17 Certification of Fair Business Practices

That the submitter affirms that the submitter has not been found guilty of unfair business practices in a judicial or state agency administrative proceeding during the preceding year. The submitter further affirms that no officer of the submitter has served as an officer of any company found guilty of unfair business practices in a judicial or state agency administrative during the preceding year.

10.18 Certification of Good Standing Texas Corporate Franchise Tax Certification

Pursuant to Article 2.45, Texas Business Corporation Act, state agencies may not contract with for profit corporations that are delinquent in making state franchise tax payments. The undersigned authorized representative of the corporation making the offer herein certified that the following indicated Proposal is true and correct and that the undersigned understands that making a false Proposal is a material breach of contract and is grounds for contract cancellation.

10.19 Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment.

Pursuant to Public Law 115-232, Section 889, and 2 Code of Federal Regulations (CFR) Part 200, including §200.216 and §200.471, NCTCOG is prohibited from using federal funds to procure, contract with entities who use, or extend contracts with entities who use certain telecommunications and video surveillance equipment or services provided by certain Chinese controlled entities. The Contractor agrees that it is not providing NCTCOG with or using telecommunications and video surveillance equipment and services as prohibited by 2 CFR §200.216 and §200.471. Contractor shall certify its compliance through execution of the “Prohibited Telecommunications and Video Surveillance Services or Equipment Certification,” which is included as Appendix D of this Contract. The Contractor shall pass these requirements down to any of its subcontractors funded under this Agreement. The Contractor shall notify NCTCOG if the Contractor cannot comply with the prohibition during the performance of this Contract.

10.20 Discrimination Against Firearms Entities or Firearms Trade Associations

Pursuant to Texas Local Government Code Chapter 2274, Subtitle F, Title 10, prohibiting contracts with companies who discriminate against firearm and ammunition industries. NCTCOG is prohibited from contracting with entities, or extend contracts with entities who have practice, guidance, or directive that discriminates against a firearm entity or firearm trade association. Contractor shall certify its compliance through execution of the “Discrimination Against Firearms Entities or Firearms Trade Associations Certification,” which is included as Appendix D of this Contract. The Contractor shall pass these requirements down to any of its subcontractors funded under this Agreement. The Contractor shall notify NCTCOG if the Contractor cannot comply with the prohibition during the performance of this Contract.

10.21 Boycotting of Certain Energy Companies

Pursuant to Texas Local Government Code Chapter 2274, Subtitle F, Title 10, prohibiting contracts with companies who boycott certain energy companies. NCTCOG is prohibited from contracting with entities or extend contracts with entities that boycott energy companies. Contractor shall certify its compliance through execution of the “Boycotting of Certain Energy Companies Certification,” which is included as Appendix D of this Contract. The Contractor shall pass these requirements down to any of its subcontractors funded under this Agreement. The Contractor shall notify NCTCOG if the Contractor cannot comply with the prohibition during the performance of this Contract.

10.22 Domestic Preference for Procurements


As appropriate and to the extent consistent with law, the CONTRACTOR should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). Consistent with §200.322, the following items shall be defined as: “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. “Manufactured products” means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

10.23 Trafficking in Persons

Contractor agrees to comply with all applicable provisions of 2 CFR §175.15. NCTCOG, the Contractor, and its subcontractors are prohibited from (i) engaging in severe forms of trafficking in persons during the period of time that the award is in effect; (ii) procure a commercial sex act during the period of time that the award is in effect; (iii) use forced labor in the performance of the award or subawards under the award. The Federal award agency may unilaterally terminate the award, without penalty, if the Contractor (i) is determined to have violated an applicable prohibition; (ii) has an employee who is determined by the agency officially authorized to terminate the award to have violated an applicable prohibition of this award term. NCTCOG must notify the Federal award agency immediately if any information received from the Contractor indicates a violation of the applicable prohibitions.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

V3Main Technologies, Inc.


 Signature Date 05/08/2025

Venkat Maddikayala
 Printed Name
President and CEO
 Title

North Central Texas Council of Governments

Signed by:
 5/14/2025
 Signature A4E72C1BEF0F426... Date
 Michael Eastland
 Executive Director

APPENDIX A

Statement of Work

The Contractor agrees to provide AI Solutions in accordance with the scope of work outlined in Request for Proposal (RFP) No. 2025-018, and as further detailed in the Contractor's technical response, which is incorporated herein and made a part of this Statement of Work.

1. The Contractor shall be responsible for the design, development, deployment, and ongoing support of customized Artificial Intelligence (AI) solutions. These solutions must:
 - a. Address and solve specified operational and strategic challenges.
 - b. Integrate seamlessly with existing agency systems and databases.
 - c. Be intuitive, user-friendly, and accessible to a broad range of stakeholders.
 - d. Include end-user training, system documentation, and ongoing support for staff.
 - e. Provide ongoing maintenance, upgrades, and compliance assurance with applicable data security and privacy standards.
 - f. Ensure data security and privacy compliance in alignment with state and federal regulations.
2. Technical Requirements

The Contractor shall ensure that all AI solutions meet the following technical specifications:

 - a. Scalability: Must support growth in both data volume and user interaction without degradation of performance.
 - b. System Integration: Solutions must integrate with existing platforms.
 - c. Security frameworks: MDM, IAM, SIEM, and related infrastructure
 - d. Real-Time Analytics: Must provide real-time data analysis and reporting.
 - e. Data Security & Privacy Compliance: Adherence to standards such as GDPR, HIPAA, and CCPA are required.
 - f. Natural Language Processing (NLP): Advanced NLP capabilities must be embedded to support diverse and accurate user interactions.
 - g. Accuracy & Validation: Contractor must demonstrate and maintain a high level of system accuracy and describe methods for validation and quality assurance.
 - h. Algorithm Transparency: Solutions must include clear documentation of AI algorithms, approaches to mitigating bias, validation processes, and explainability.
 - i. Continuous Improvement: Solutions must include features for ongoing learning, with mechanisms to incorporate feedback and improve performance over time.
 - j. Interoperability: AI systems must comply with open standards and be capable of integrating with current and future digital infrastructure.
 - k. Quality Control: Contractor shall maintain rigorous quality control protocols to ensure consistent and reliable system performance.
3. Data Governance

The Contractor must implement the following data governance practices:

 - a. Data Integrity and Accuracy: Ensure reliable data quality through lifecycle validation checks and automated error correction.
 - b. Data Privacy Compliance: Adhere to all relevant privacy laws. Implement data anonymization and pseudonymization as needed and obtain/document user consent for data collection and use.
 - c. Access Controls: Implement role-based access controls and multi-factor authentication (MFA) for all sensitive data access.
 - d. Data Retention and Disposal: Define and adhere to policies for secure data retention and disposal.
 - e. Data Auditing and Monitoring: Regular auditing must be conducted, and access/modification logs must be maintained and made available upon request.
4. Cybersecurity Requirements

The Contractor shall maintain strong cybersecurity practices throughout the contract period:

 - a. Threat Detection & Response: Deploy AI-based threat detection tools. Define incident response plans and test them regularly.
 - b. Encryption: Utilize end-to-end encryption (AES-256, RSA-2048, etc.) for both data in transit and at rest.

- c. Vulnerability Management: Perform regular security assessments and penetration testing. Patch vulnerabilities promptly.
- d. Security Governance Framework: Establish and follow a documented governance model with defined policies, controls, and responsibilities.
- e. Risk Management: Identify risks, establish mitigation strategies, maintain a disaster recovery plan, and conduct root-cause analysis following incidents.
- f. Training & Awareness: Provide regular cybersecurity training to all relevant agency staff. Training must address both technical procedures and general awareness.

Artificial Intelligence (AI) Solutions for Public Sector Entities**1 Executive Summary**

Proven Track Record of implementing Cybersecurity for TX Government: Demonstrated history of implementing large-scale cybersecurity solutions for Texas state agencies, including SOC modernization, Zero Trust Architecture, and hybrid cloud-native applications, ensuring robust operational and security frameworks.

- **Advanced Cybersecurity Solution: CyberPod AI:** Powered by state-of-the-art Large Language Models (LLMs), CyberPod delivers proactive threat detection, automated compliance, and vulnerability prioritization. It integrates seamlessly into workflows, enabling actionable insights, reduced manual efforts, and advanced orchestration for Texas agencies.
- **Seamless Integration with Legacy Systems:** CyberPod integrates effortlessly with existing platforms, maintaining operational continuity. Its modular, scalable architecture allows it to grow with organizational needs, adapting to evolving threats while enhancing interoperability with tools like SIEMs and cloud systems.
- **Cost-Effective and Scalable Architecture:** By automating repetitive tasks and optimizing workflows, CyberPod reduces manual intervention and external dependencies, delivering up to 50% cost savings. Its scalable framework ensures long-term adaptability for both immediate and future challenges.
- **Comprehensive Cybersecurity Expertise:** Our dedicated team of 50+ cybersecurity consultants brings unmatched expertise across critical areas such as threat intelligence, vulnerability management, endpoint protection, and disaster recovery. With decades of collective experience, our team has successfully implemented advanced frameworks like Zero Trust Architecture and AI-powered threat hunting, ensuring proactive and resilient security postures. Additionally, we deliver tailored security training programs designed to enhance workforce readiness, reducing incident risks by 20% and empowering organizations to effectively mitigate evolving threats.

2 Technical Approach**2.1 Objectives of the RFP**

The primary objective of this RFP is to enhance the cybersecurity capabilities of the Texas government by leveraging advanced technologies to address current challenges. This includes improving threat detection and mitigation, automating repetitive processes, enhancing collaboration across departments, and ensuring data integrity and privacy for critical state infrastructure.

2.2 Scope of the RFP

- Strengthen the state's cybersecurity posture by integrating AI-driven solutions.
- Automate processes for threat detection, vulnerability management, compliance, and incident response.
- Provide continuous monitoring and proactive risk assessment.
- Foster collaboration across state departments to ensure unified cybersecurity efforts.
- Deliver training and support to ensure seamless adoption of the proposed solution.

Artificial Intelligence (AI) Solutions for Public Sector Entities**2.3 Key Challenges**

Texas government agencies, like their counterparts across the U.S., face several cybersecurity challenges:

- **Ransomware Attacks:** Frequent and sophisticated attacks disrupt essential services, as demonstrated by recent cases where ransomware campaigns targeted public utility systems, halting operations and risking public safety.
- **Talent Shortage:** Difficulty recruiting and retaining cybersecurity professionals due to competition with the private sector. The gap in skilled personnel delays implementation of proactive cybersecurity strategies.
- **Legacy Systems:** Outdated infrastructure increases vulnerability to attacks. Legacy database vulnerabilities identified in past Texas government audits showed how system incompatibilities hinder security patching.
- **Fragmented Security Operations:** Disconnected systems and tools hinder comprehensive threat management. For example, multiple departments using isolated SIEM systems face challenges in unified threat correlation and response.
- **Data Breaches:** Protecting sensitive citizen data is increasingly complex due to evolving regulations. Instances of incomplete data encryption practices have exposed personally identifiable information (PII).
- **Compliance Management:** Staying compliant with federal and state cybersecurity mandates is resource-intensive. Manual compliance reporting in some departments increases overhead and error rates.
- **Insufficient Monitoring:** Lack of continuous monitoring leaves critical assets exposed. A state audit revealed gaps in monitoring third-party vendor access, posing significant risks to sensitive systems.
- **Emerging Threats:** New challenges include supply chain attacks, where compromised software vendors provide an entry point for threat actors. This growing issue requires advanced detection capabilities.

2.4 Current Technologies and Pain Points

- **Technologies in Use:**
 - Firewalls, Intrusion Detection Systems (IDS), and Security Information and Event Management (SIEM) tools.
 - Endpoint Protection Platforms (EPPs) and Vulnerability Management solutions.
 - Legacy databases and disparate tools for asset and risk management.
- **Pain Points:**

Artificial Intelligence (AI) Solutions for Public Sector Entities

- Limited interoperability among tools, leading to silos.
- High maintenance costs for legacy systems.
- Inefficient manual processes for compliance and incident documentation.
- Delays in threat detection and response due to fragmented workflows.

2.5 Opportunities for AI Solutions

AI offers transformative opportunities to address these challenges:

- **Automated Threat Detection and Response:** Proactively identify and neutralize threats in real time.
- **Vulnerability Prioritization:** Use AI to assess and rank vulnerabilities based on risk.
- **Improved Collaboration:** Foster seamless integration between security tools and teams.
- **Enhanced Efficiency:** Automate manual tasks like compliance reporting and shift handovers.
- **Proactive Risk Assessment:** Use predictive analytics to anticipate and mitigate risks.

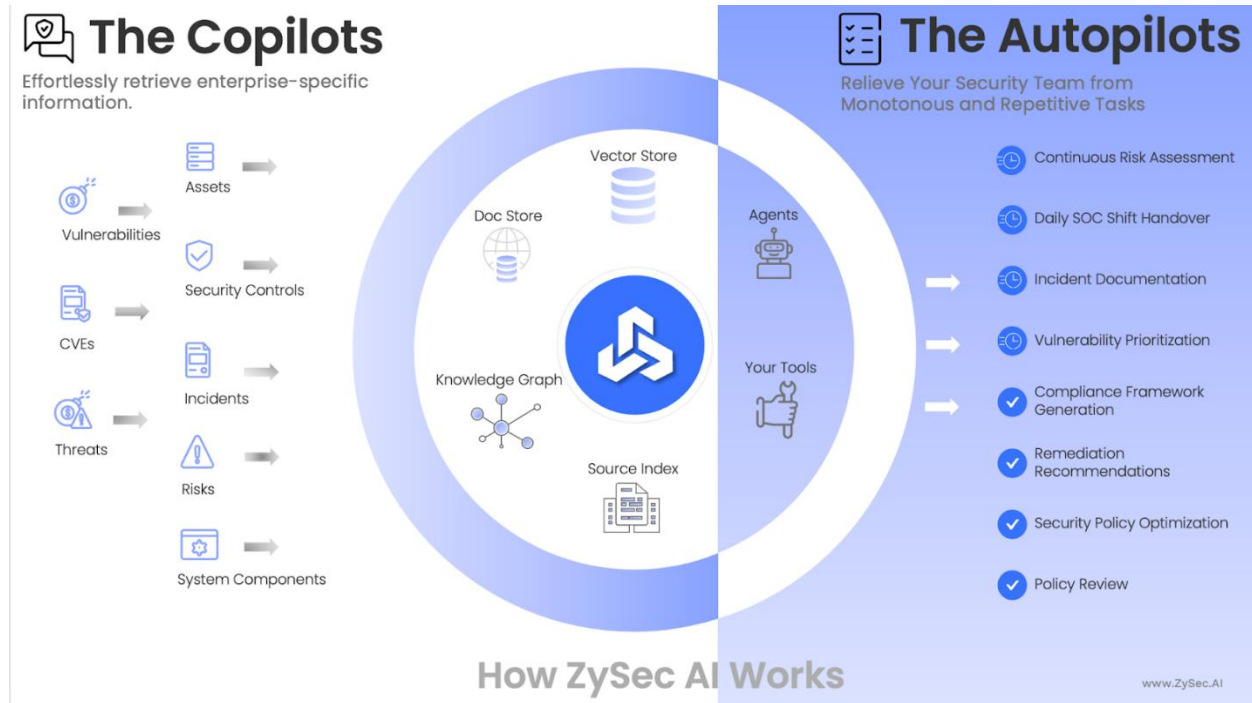
2.6 Key Considerations for the AI Solution

- **Interoperability:** Must seamlessly integrate with existing tools and technologies.
- **Data Privacy and Ownership:** Ensure data remains within the government's control.
- **Scalability:** Adapt to growing data volumes and evolving threats.
- **Ease of Use:** Provide intuitive interfaces and minimize the learning curve.
- **Customizability:** Tailor AI capabilities to address specific departmental needs.
- **Security:** Be designed with robust measures to ensure system integrity and confidentiality.

3 Introducing CyberPod AI

CyberPod AI: Autonomous Enterprise Security

Introducing CyberPod AI, an autonomous platform powered by advanced AI for enterprise security. CyberPod deploys a network of intelligent AI agents that operate independently yet in perfect coordination, redefining how enterprises secure, manage, and optimize their digital operations.



CyberPod AI seamlessly integrates with your existing operations, creating a dynamic security ecosystem that adapts to your enterprise evolving needs. Its autonomous agents optimize various aspects of your digital landscape—from proactive threat management, operational efficiency and compliance management supporting strategic decision making.

CyberPod AI leverages advanced AI to detect compliance gaps, risks, and security threats before they arise. With continuous compliance monitoring, real-time risk assessments, and adaptive governance that keeps pace with changing regulations, CyberPod AI ensures your enterprise stays secure and compliant.

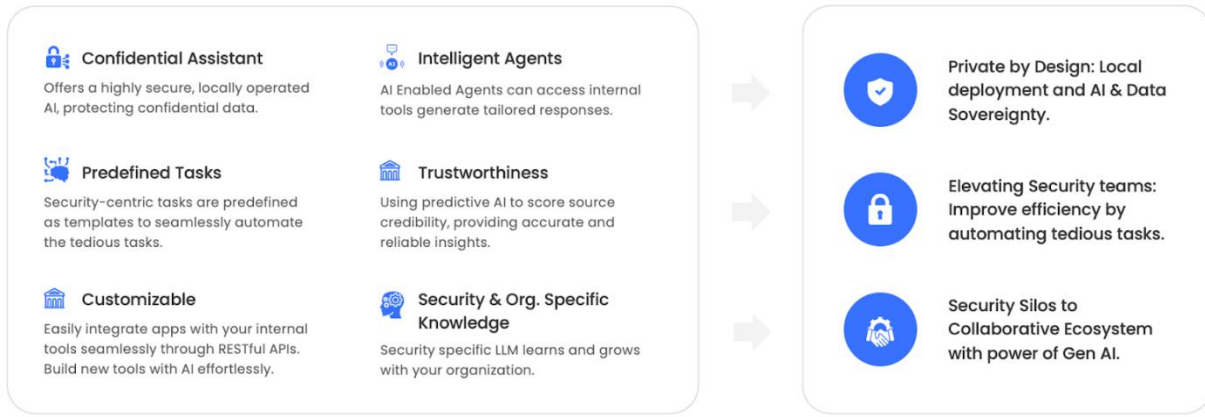
In today's digital landscape, CyberPod AI stands as your trusted security ally, tirelessly defending your enterprise. By deploying CyberPod AI, you're not just adopting a tool—you're integrating AI and creating AGI for your enterprise security. This autonomous system seamlessly extends your security workforce, proactively protecting your digital assets around the clock. Leverage the power of AI and autonomous agents to revolutionize your security posture and strengthen your operational resilience. The future of enterprise security isn't just envisioned—it's realized, here and now, with CyberPod AI. Experience the transformation today.

3.1 Product Overview

CyberPod AI is a transformative, AI-centric platform designed to seamlessly integrate into existing ecosystems. It doesn't replace your current tools but enhances them by acting as an intelligent orchestration layer. With adaptability at its core, CyberPod evolves with your

Artificial Intelligence (AI) Solutions for Public Sector Entities

organization's needs, providing actionable insights, unifying data from diverse systems, and empowering decision-makers to stay future-ready.



Capabilities and Benefits

- **Unified Threat and Security Posture:** Aggregates data from various systems and subsystems to present a comprehensive, real-time view of your organization's security landscape.
- **Seamless Ecosystem Integration:** Connects effortlessly with existing tools and platforms, enhancing their utility without disrupting current workflows.
- **AI-Driven Contextual Insights:** Leverages advanced AI to provide actionable, context-aware intelligence tailored to your organizational environment.
- **Adaptable and Scalable Design:** Evolves with your organization's needs, ensuring long-term relevance and value as your infrastructure grows.
- **Collaborative Security Framework:** Facilitates cross-functional collaboration by centralizing insights and enabling teams to work together with shared, actionable data.
- **Dynamic Decision Support:** Provides leaders with data-driven recommendations to make informed, proactive decisions aligned with strategic priorities.
- **Operational Efficiency at Scale:** Orchestrates processes across systems, streamlining workflows and reducing operational complexity without duplicating efforts.

Future-Ready AI Platform Equips organizations with an AI-powered toolkit to proactively address emerging threats and evolving cybersecurity challenges.

Artificial Intelligence (AI) Solutions for Public Sector Entities**Use cases**

Unlock the power of CyberPod AI with an extensive range of security use cases designed to tackle the toughest challenges across diverse domains, delivering actionable intelligence and transformative results.

NIST – CYBER SECURITY FRAMEWORK					
GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Risk Management and reporting	Risk assessment (Internal, third party, supply chain etc.)	Cloud Security	Threat research (Attack surface management, TI analysis, Vuln. impact assessment)	Security Incident Handling, RCA and Incident reporting	Incident Recovery Planning
Legal review Data protection and privacy assessment	Regulatory & Compliance Management (CIS, FedRAMP, PCI-DSS, ISO etc.)	Application Security	Security Alert Triage and Analysis, Threat Hunting	Cyber Drill Table-Top Exercise	Lessons learned report
Security Policy Generation	Architecture Review	Identity & Access reviews		Incident Reporting and Documentation	
Situational Report Security Strategy	Threat Modeling				

Artificial Intelligence (AI) Solutions for Public Sector Entities

Note: The listed use cases are only a subset. The platform supports a much broader range of use cases and is highly customizable around your policies, tools and learnings.

3.2 How CyberPod AI and V3Main Experience Address Challenges:**1. Enhanced Threat Detection and Response:**

- CyberPod AI integrates predictive analytics with V3Main's proven threat management techniques to ensure rapid identification and neutralization of threats. This synergy optimizes security operation centers (SOCs) by automating real-time threat detection.

2. Automation Across Security Operations:

- Routine tasks such as compliance documentation, vulnerability assessments, and incident reporting are automated using CyberPod's predefined templates. V3Main's domain expertise ensures these templates align with Texas government's specific requirements.

3. Vulnerability Prioritization and Remediation:

- CyberPod AI's advanced risk assessment models, combined with V3Main's experience in vulnerability management for Texas government systems, streamline the prioritization and resolution of critical vulnerabilities.

4. Seamless Integration with Existing Systems:

- With V3Main's deep understanding of legacy systems and CyberPod's flexible APIs, the solution integrates effortlessly with existing tools like SIEMs and firewalls, ensuring continuity and enhanced functionality.

5. Continuous Monitoring and Risk Assessment:

- CyberPod AI and V3Main's monitoring frameworks provide comprehensive 24/7 oversight of critical assets. This dual approach leverages historical and real-time data to proactively identify risks.

6. Customized Insights and Collaboration:

- CyberPod AI's Copilot features, supported by V3Main's insights into state-specific cybersecurity needs, enable tailored advice for different government departments. This fosters interdepartmental collaboration and informed decision-making.

7. Data Sovereignty and Privacy:

V3Main Technologies **RFP-2025-018** **www.v3mainglobal.com**
Artificial Intelligence (AI) Solutions for Public Sector Entities

- CyberPod AI ensures all data remains within Texas' jurisdiction, aligning with V3Main's established data privacy protocols for government systems. This guarantees compliance with state and federal regulations.

3.3 Key Differentiators

Modular, Containerized Architecture

Highly modular, containerized design reduces operational overhead and allows seamless switching between components, ensuring flexibility and scalability.

Localized and Air-Gapped by Design ensures Data Sovereignty

Fully localized platform with air-gapped deployment ensures security by design, aligning with organizational and regional regulatory standards, ensures Data Sovereignty.

Regulatory Compliance Ready

Designed to seamlessly adapt to frameworks like PCI DSS, SOC 2, and GDPR, leveraging modern components to integrate compliance into every deployment phase.

Specialized Cybersecurity Models

Purpose-built, lightweight models focus on specific cybersecurity tasks, optimizing token costs while maintaining exceptional performance.

Effortless Usability for All Teams

Intuitive interface designed for both technical and non-technical users, enabling rapid adoption and effective use without specialized training.

Scalable to Organizational Needs

Adaptable to evolving business requirements, with microservices that integrate seamlessly into existing infrastructures.

Cost-Effective Operations

Minimizes dependency on external consultants and streamlines processes, delivering high-value outputs at significantly reduced costs.

AI-First Security Orchestration

Acts as a unifying layer, connecting with existing tools to provide actionable insights and orchestrated workflows without replacing existing systems.

3.4 Organizational Impact

CyberPod AI transforms the way organizations approach security by introducing AI-Driven Agents and an Enterprise Security Orchestration Platform (ESRP) designed for seamless adaptability. These intelligent agents act as co-pilots, delivering context-aware insights, automating repetitive tasks, and streamlining decision-making. By embedding organizational policies and leveraging existing tools and workflows, CyberPod creates a unified, adaptable framework that enhances security operations without disrupting existing infrastructure.

Today	With ZySec AI
Security teams - Referencing assets and incidents.	Reduces time spent on referencing tools by 70% .
Security architects and compliance teams - Making policies by referencing various sources, continuous monitoring.	Cuts policy reference and monitoring time by 50% .
Vulnerability management - Tracking external CVEs, vulnerabilities prioritization.	Simplifies vulnerability tracking and reduces effort by 65% .
SOC Teams – Shift handovers, report generation.	Streamlines shift handovers and report generation, saving 60% of time.

With its modular, scalable architecture, CyberPod evolves alongside your organization, ensuring it aligns with regulatory standards, protects data sovereignty, and drives cost efficiency. It functions as a seamless layer that integrates effortlessly into your ecosystem, connecting disparate systems and workflows into one cohesive and intelligent operation.

Tedious tasks are accomplished at scale.

Security Ticket Review:

Evaluate security compliance of each ticket against standards, taking 10 minutes per ticket, with at least 10 tickets processed daily.

Incident Reporting:

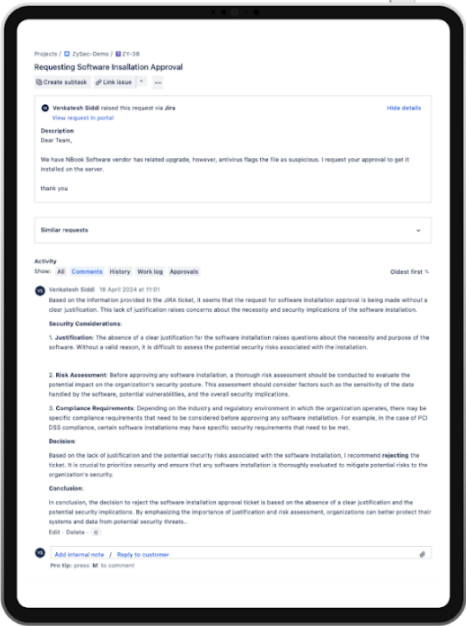
Update incident reports with tailored details, appx. 8 minutes per incidents for about 50 incidents a day.

Threat Intelligence Synthesis:

Aggregate newsletters synthesis daily intel brief generate internal review tickets, saving approximately 20 minutes per day.

Vulnerability Prioritization:

Review assets against new CVE entries and generate actionable tickets, spending 30 minutes on each of about 10 monthly tickets.



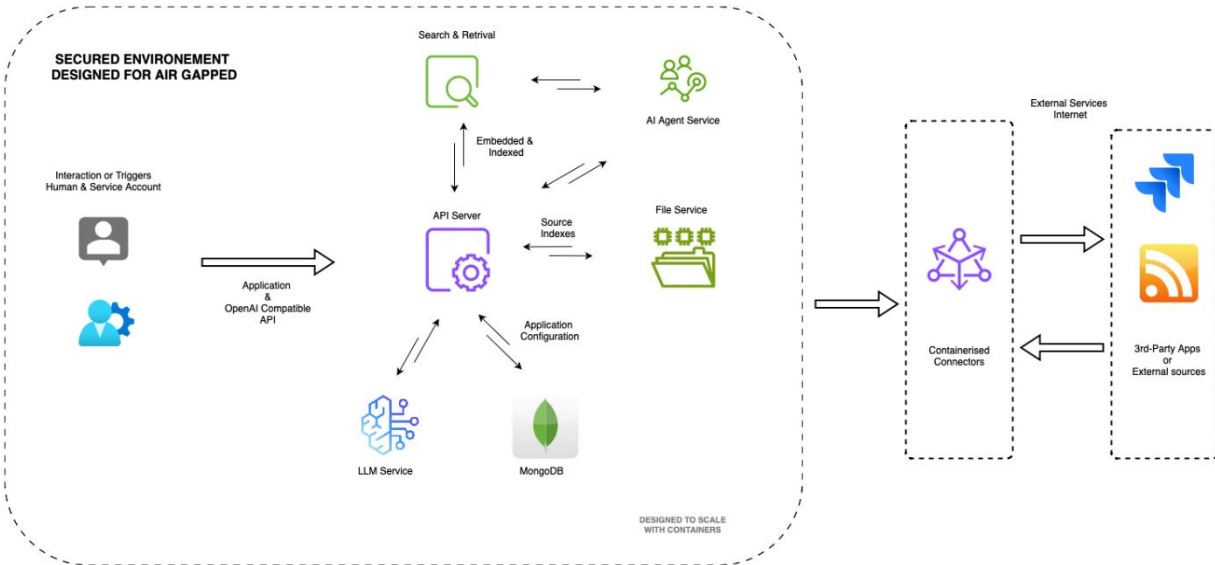
This platform empowers security teams to act with precision, make faster decisions, and focus on strategic priorities. It fosters innovation by transforming organizational security into an agile, future-ready framework capable of addressing modern challenges. CyberPod AI goes beyond incremental improvements—it lays the foundation for a forward-thinking, AI-driven security strategy that maximizes efficiency, ensures compliance, and strengthens collaboration.

CyberPod AI is more than a solution; it’s an enabler of transformation, preparing organizations to tackle evolving threats and giving security leaders the tools to lead their teams with confidence in an AI-powered era.

4 Deployment and Integration

CyberPod AI is built to process both structured and unstructured data, providing advanced capabilities in data processing, entity recognition, and AI-driven analysis. Designed for seamless integration, it aligns with operational workflows and supports the consolidation of diverse data sources into meaningful and actionable insights. This scalable and adaptable system ensures enhanced investigative efficiency, supports informed decision-making, and operates fully on-premises with a secure, isolated external connection mechanism to protect your sensitive data.

Artificial Intelligence (AI) Solutions for Public Sector Entities



- **Scalable Pipelines:** Enables progressive data ingestion and seamless integration of new data sources over time.
- **Localized Deployment:** Fully localized infrastructure to comply with regional data security and privacy regulations.
- **Knowledge Graph Building:** Creates dynamic relationships between entities for enhanced contextual understanding.
- **State-of-the-Art RAG System:** Integrates retrieval-augmented generation for accurate and efficient knowledge discovery.
- **Advanced Processing Pipelines:** Includes chunking, embedding, and analysis workflows for efficient data handling.
- **Specialized Models for security:** Fine-tuned AI models tailored to meet the specific needs of security.
- **Source Attribution Capabilities:** Ensures accurate and reliable information by tracking data sources and scoring their credibility.

4.1 Solution Delivery

The delivery of the solution will be carried out in a phased and systematic manner to ensure seamless implementation, customization, and alignment with the customer's requirements. The approach is structured as follows:

Phase 1: Requirement Analysis and Feasibility Study

V3Main Technologies **RFP-2025-018** **www.v3mainglobal.com**
Artificial Intelligence (AI) Solutions for Public Sector Entities

- Conduct detailed discussions with stakeholders to finalize requirements and identify any feasibility challenges.
- Perform technology readiness assessments and define success metrics for the initial deployment.

Phase 2: Solution Design and Customization

- Adapt the CyberPod solution to meet customer-specific use cases.
- Customize workflows, pipelines, model training and guardrails to align with operational needs.

Phase 3: Development and Deployment

- Implement scalable, containerized components for data processing, model deployment, and AI-driven workflows.
- Deploy AI Agentic tasks with Autopilot functionality, ensuring modularity for future adjustments.

Phase 4: Testing and Validation

- Perform comprehensive testing, including functional, security, and user acceptance testing (UAT).
- Validate performance metrics to ensure alignment with customer expectations and operational goals.

Phase 5: Training, Handover, and Support

- Deliver training sessions to familiarize end-users with the solution and its workflows.
- Conduct a formal handover meeting to finalize and document the first phase's deliverables.

Provide ongoing operational and maintenance support, along with periodic reviews to ensure system optimization.

4.2 Our Experience and Credentials

Parabola9 and V3Main Technologies have a combined track record of delivering robust cybersecurity solutions to government and enterprise clients. Highlights include:

- Comprehensive SOC Modernization: Upgraded and automated Security Operations Centers (SOCs) for various Texas government departments, reducing incident response times by 40%. Leveraged advanced SIEM integration and automated alert triaging to streamline workflows.

Artificial Intelligence (AI) Solutions for Public Sector Entities

- **Proactive Risk Assessment:** Deployed predictive analytics models and machine learning tools to identify and mitigate risks proactively across critical state infrastructure. Improved visibility into real-time threat landscapes and enabled actionable intelligence for decision-makers.
- **Vulnerability Management:** Streamlined vulnerability assessment and prioritization processes for legacy systems using advanced AI-driven prioritization algorithms, ensuring faster remediation of critical risks. Reduced patch deployment time by 30% while ensuring compliance.
- **Compliance Expertise:** Implemented automated compliance reporting frameworks tailored to state and federal mandates. Achieved a 50% reduction in manual effort for reporting processes while ensuring 100% audit readiness.
- **Advanced Threat Detection Systems:** Delivered tailored AI-driven threat detection solutions that integrate seamlessly with existing government systems, providing real-time alerts and enhancing overall situational awareness.
- **Incident Response Frameworks:** Designed and deployed standardized incident response frameworks to improve coordination across multiple departments. Implemented automated incident logging and escalation workflows, improving response times by at least 25%.
- **Customized Security Training:** Delivered specialized training programs for state employees to enhance cybersecurity awareness and operational readiness, reducing human-error-related incidents by 20%.
- **Implement a zero trust security model** where no one, inside or outside the network, is trusted by default. Continuous verification of user and device identities helps protect against unauthorized access. Improve security landscape and prevent ransomware attacks sooner than later.
- **Disaster and Recovery:** Enterprise Data Security using industry best practices related to encryption, decryption, cloud native backup and recovery solutions. Improve RPO and RTO by 30%

4.3 Our Key Differentiator

- **Tailored AI Expertise:** Customized solutions leveraging domain-specific large language models (LLMs).
- **End-to-End Automation:** Automates the entire cybersecurity lifecycle from detection to remediation.
- **Privacy-First Approach:** Locally deployed solutions ensure data sovereignty.

V3Main TechnologiesRFP-2025-018www.v3mainglobal.com

Artificial Intelligence (AI) Solutions for Public Sector Entities

- **Collaborative Partnerships:** Leveraging V3Main’s deep expertise in Texas government’s cybersecurity landscape.
- **Proven Impact:** Demonstrated ability to reduce costs and improve efficiency across various cybersecurity functions.

By integrating CyberPod AI with the expertise of V3Main Technologies, the Texas government can achieve a robust, proactive, and efficient cybersecurity posture, ensuring the safety and integrity of its critical systems and data.

4.4 CyberPod AI Implementation Approach

High Level Project Plan (Indicative)

The following graph illustrates the high level project plan of CyberPod AI solution.

	W1	W2	W3	W4	W5	W6	W6..	Y1	Y2	Y3..
Phase 1: Requirement Analysis and Feasibility Study										
Phase 2: Solution Design and Customization										
Phase 3: Development and Deployment										
Phase 4: Testing and Validation										
Phase 5: Training, Handover										
Operations Support										

Note: The timeline is highly dependent on customer objectives, above are listed for solution design and deployment with minimal customization.

Key Milestones and Deliverables

Artificial Intelligence (AI) Solutions for Public Sector Entities

S. No	Key Milestone	Activities	Deliverables
1	Requirement gathering	Detailed requirement gathering, detailed project plan	Detailed requirement document
2	Data Exploration	Review datasets, and build relationships to enrich investigations, generate knowledge graph.	Knowledge graph
3	Model Fine-tuning and Customization	Fine-tune LLMs and embeddings to ensure optimal performance for customer tasks.	Fine tuned LLM
4	CyberPod AI Deployment	Installation, customization, testing of solution.	Cyberpod AI deployed in customer premises
5	Autopilot Development & deployment	Autopilots with given use cases will be deployed	Autopilot use cases deployed
6	Training & documentation	Provide training & documentation	Provide end user training Handover the platform related documentation
7	AI Advisory, AI Security Consulting & Support	Product support On-demand AI advisory & consulting.	On Demand, Time and material pricing as per project.

Artificial Intelligence (AI) Solutions for Public Sector Entities**Service Governance**

The implementation of the project will include a structured schedule of daily, weekly, and bi-weekly meetings to ensure effective communication, progress tracking, and alignment among all stakeholders.

- **Daily Task Updates:** These meetings provide updates on task progress, highlighting completion percentages, challenges, and dependencies. They ensure immediate resolution of blockers to maintain the project's momentum.
- **Weekly Progress Report Meetings:** These sessions focus on detailed status updates, accomplishments from the past week, and tracking progress against the baseline plan. They also review project risks, dependencies, and actions for the next steps, while determining if escalations are required.
- **Bi-Weekly Executive Steering Committee Meetings:** These high-level meetings involve leadership updates, directional guidance, and reviews of executive status reports. They address escalated risks, align policies, and manage relationships to ensure strategic alignment and project success.

4.5 Key Personnel and Resume**4.5.1 Venkat Maddikayala, PMP, Enterprise Architect/Scrum Master/Contract Administrator/Project Manager**

Over 29+ years of experience managing the IT projects using Waterfall, Agile and Scrum Methodologies. Oversee the overall execution of the TxShare Projects and provide, AI related Architecture , Design and implementation of AI solutions to the end clients.

Profile 1: Senior Cybersecurity Consultant, brings over 12 years of experience in implementing and managing advanced security solutions for regulated industries and air-gapped environments. He has expertise in AI-powered security platforms, including LLM-based solutions, security operations automation, and process optimization. He is well-versed in regulatory compliance standards such as GDPR, HIPAA, and ISO 27001, and he has extensive experience integrating third-party tools with enterprise systems. Among his accomplishments, he has successfully led teams to develop workflows that reduced response times by 30% and provided training on AI-driven platforms to enhance security team capabilities. In the context of CyberPod AI, he leads the deployment and customization of the platform, ensures seamless integration with organizational workflows, and trains teams to maximize the platform's potential

Profile 2: AI Security Specialist, has 10 years of experience in designing and deploying AI-driven security solutions tailored to industry-specific needs. Her expertise includes the design and tuning of on-premises LLMs, building AI agents for security operations, ensuring data sovereignty, and customizing user workflows. He has a proven track record of enhancing threat detection accuracy by 25% for a financial institution through tailored AI models and automating repetitive tasks, saving over 1,000 hours annually for security teams. He has also delivered AI

Artificial Intelligence (AI) Solutions for Public Sector Entities

solutions in air-gapped environments that comply with strict regulations. For CyberPod AI, he specializes in customizing LLMs to meet organizational security needs, configuring AI agents to address operational challenges, and providing ongoing support to ensure the platform's long-term success.

4.6 Program/Project Management

Our program management philosophy is based upon exceeding our customers' expectations while ensuring that we treat our employees as valuable assets. To that end, our approach emphasizes strong leadership focused on client success, with a thorough understanding of our client's needs, desires, and limitations. It also emphasizes openness and cooperation among our employees, subcontractors, clients, and other stakeholders, as well as continuous process improvement, and short-term problem resolution. This enables us to provide a fast and effective responses to any immediate problems as required, as well as the ability to implement systemic improvements. This will lead to higher productivity, increased system reliability, and user satisfaction.

For Artificial Intelligence (AI) Solutions for Public Sector Entities ("AIS-PSE"), V3MAIN will implement a Program Management Office (PMO) to support the wide variety of development, implementation, and operational support needed to meet the TxShare's requirement for support of the AIS-PSE. Our PMO, headed by V3Main's Program Manager and Contract administrator, will support the critical components needed to ensure the success of the TxShare's AIS-PSE, including:

- Coordinate project execution with all project stakeholders as defined per TO.
- Comply with the specific Intellectual Property (IP) rights/licensing for any delivered product/solutions identified in the task order to enable the Government to fully utilize the deliverable for its intended purpose
- Execute the task order and, where appropriate, provide and support recommended solutions for hosting any necessary data, algorithms, or computer infrastructure as specified in the task order.
- Task order will conduct media coordination and outreach, where appropriate, to advertise task order defined projects and build participation and engagement.
- holding scheduled Program Management Reviews;
- providing and maintaining a Project Plan
- maintaining a Master Program Schedule and Calendar for the program;
- providing Risk and Safety Management to mitigate potential negative outcomes;
- implementing ISO 9001 and the DoD approved Quality Management processes;
- performing Configuration Management (CM) on applicable program components;
- implementing a Performance Plan to monitor and assess project performance;
- implementing an effective User Support Management process to ensure customer satisfaction;
- performing robust Document Management for all TxShare artifacts; and,
- Providing monthly status reports;
- Executive reports involving incidents, dashboards for systems status performance, and infrastructure report cards;

As a part of our PMO support, V3MAIN will provide the following deliverables for the TxShare's AIS-PSE Task Order project:

- Contract Kickoff Meeting – V3MAIN will hold a TO contract kickoff meeting within 10 days of contract award to facilitate the introduction of all TxShare and V3MAIN stakeholders
- Plans for each of the TO requirements defined in the scope
- Provisions for validating that SOW requirements are met
- Issue identification, tracking, and resolution
- Staffing plans (including provisions for workload fluctuations cost monitoring and management processes)
- An organizational chart; and, a communications plan, QA plan, CM plan
- Master Program Schedule and Calendar
- Risk Register
- User Support/Issue Tracking System
- Monthly Status Reports

5 Cybersecurity Best Practices and Tools

V3Main has partnered with Parabola9 to deliver comprehensive AI-driven solutions. Together, we bring extensive experience in implementing AI-based cybersecurity solutions for Texas agencies. Currently, V3Main is engaged with the Texas government through Texas DIR contracts for cybersecurity products and services. Our contributions include providing enterprise architecture to the Texas Comptroller of Public Accounts (CPA), which involved implementing Zero Trust Architecture frameworks, cloud-native solutions leveraging microservices, API gateways, and DevSecOps practices. We are well-versed in TxRAMP policies and ensure that our solutions fully comply with TxRAMP requirements.

5.1.1 Regular Software Updates:

Ensure that all software, including operating systems, applications, and firmware, is regularly updated. Vendors often release patches that address known vulnerabilities.

As part of IT Managed Services, V3Main has partnered with several Patch Management service providers. Some of the V3Main Vendors are:

Microsoft, Datto RMM, Cisco, Fortinet, Red hat Ansible Automation, Solar Winds and Barracuda

We constantly evaluate various vendors to meet our client requirements.

5.1.2 Intrusion Detection and Prevention Systems (IDPS):

Implement IDPS to monitor network traffic for suspicious activity and potential exploits. These systems can help detect and block zero-day attacks.

Artificial Intelligence (AI) Solutions for Public Sector Entities

Signature-based Detection: It uses uniquely identifiable signatures that are located in exploit code. When exploits are discovered, their signatures go into an increasingly expanding database. Signature-based detection for IPS involves either exploit-facing signatures, which identify the individual exploits themselves, or vulnerability-facing signatures, which identify the vulnerability in the system being targeted for attack. Vulnerability-facing signatures are important for identifying potential exploit variants that haven't been previously observed, but they also increase the risk of false positive results (benign packets mislabeled as threats).

Statistical Anomaly-based Detection: This randomly samples network traffic and compares samples to performance level baselines. When samples are identified as being outside the baseline, the IPS triggers an action to prevent a potential attack.

Host-based IDPS might monitor wired and wireless network traffic, system logs, running processes, file access and modification, and system and application configuration changes. Most host-based IDPSs have detection software known as agents installed on the hosts of interest.

Tools: Cisco Secure IPS, FortiGate IPS , SolarWinds Security Event Manager, Azure Firewall IDPS , AlienVault USM, and Snort

We constantly evaluate various vendors to meet our client requirements

5.1.3 Endpoint Protection:

Use advanced endpoint protection solutions that include behavior-based detection to identify and mitigate suspicious activities that may indicate a zero-day exploit.

We implement the Anti-virus, Endpoint detection and response (EDR)/ Extended detection and response (XDR), and Enterprise Data Protection solutions.

Tools: Microsoft Defender for Endpoint (MDE), Bitdefender, Threat locker, FortiXDR, Thales Cyber Trust Manager, Sentinel One, Cisco

We constantly evaluate various vendors to meet our client requirements.

5.1.4 Network Segmentation:

Divide your network into segments to limit the spread of an attack. This way, even if one segment is compromised, the attacker cannot easily access the entire network.

V3Main implements Network segmentation by dividing a network into smaller subnets.

This allows for more granular control over traffic flow and security.

Benefits

Security: Prevents unauthorized access to sensitive data, such as financial records and intellectual property

Performance: Improves network performance and reduces compliance scope

V3Main Technologies **RFP-2025-018** **www.v3mainglobal.com**
Artificial Intelligence (AI) Solutions for Public Sector Entities

Monitoring: Helps identify and fix technical issues

Isolation: Limits the spread of malware and other threats

Tools: Cisco Secure Workload, Meraki SD WAN, Fortinet FortiPolicy, VMware NSX

We constantly evaluate various vendors to meet our client requirements.

5.1.5 Application Whitelisting:

Only allow approved applications to run on your systems. This can prevent unauthorized and potentially malicious software from executing.

V3Main Implements the Application whitelisting tools like Threat locker and VMware Carbon Black which applications are allowed to run on a system. They can help prevent malware infections and ransomware attacks.

We constantly evaluate various vendors to meet our client requirements.

5.1.6 User Education and Training:

Educate employees about phishing and social engineering tactics. Awareness can help prevent attackers from gaining initial access through human error.

V3Main provides Security Awareness Training and Simulation to the V3Main Employees and Contractors

Tools: Microsoft Phishing simulation tools, KnowBe4, Barracuda

We constantly evaluate various vendors to meet our client requirements.

5.1.7 Regular Security Assessments:

Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in your systems.

We use NIST 800-30 Cyber Security Risk assessment standards and guidelines to conduct audits. We conduct internal self-assessment and external audits through third party.

Tools: Tenable, Arctic Wolf, Rapid7 Nexpose, Microsoft Defender, Vanta, Kesaya Vonai

We constantly evaluate various vendors to meet our client requirements.

5.1.8 Backup and Recovery Plans:

Maintain regular backups of critical data and have a robust recovery plan in place. This ensures that you can quickly restore operations in the event of an attack.

V3Main develop and maintain the backup and recovery procedures related to business operations, IT Systems and Disaster Recovery.

V3Main Technologies **RFP-2025-018** **www.v3mainglobal.com**
Artificial Intelligence (AI) Solutions for Public Sector Entities

Tools: Rubrik, Veeam, Trilio Vault , Pure Storage, Cloud native backup and services offered by cloud providers AWS, Azure, Google , Oracle and IBM.

We constantly evaluate various vendors to meet our client requirements.

5.1.9 Threat Intelligence:

We will monitor and inform you about the latest threats and vulnerabilities by implementing the threat intelligence solutions using the following tools

Tools: Microsoft Defender XDR, Microsoft Sentinel, Imperva, Threat Locker MDR, FortiXDR/MDR. SolarWinds SEM, Cisco Umbrella/Splunk. Sentinel One XDR, Barracuda XDR, Datto MDR, Palo Alto Cortex XSOAR Threat Intelligence Management

We constantly evaluate various vendors to meet our client requirements.

5.1.10 Zero Trust Architecture:

Implement a zero trust security model where no one, inside or outside the network, is trusted by default. Continuous verification of user and device identities helps protect against unauthorized access.

We implement Identity and Access Management, RBAC, SASE, Micro segmentation and Single Sign On to protect access to the IT Resources for User, Device, Network & Environment, Application & Workload, Data, Automation & Orchestration, and Visibility & Analytics.

Tools: Microsoft Defender for Cloud Apps, Fortinet Universal ZTNA, Cato SASE, HPE Aruba, Cisco Umbrella, Akamai EAA, OKTA SSO, Microsoft Entra, Ping Identity, Google IDP, AWS IAM, and F5 Distributed Cloud

6 Past Performance

6.1 History of the proposer

V3Main Technologies was incorporated in March 2007 in Texas. Previously, the company was called ViTech Systems but was renamed to align its business strategy. We believe it is necessary to have the right Technology, People, and Business to run any business. To this end, our company was formed to bridge the gap between business and technical knowledge by creating visibility between strategic IT and business strategic goals. Our company will bring together business and technology leaders to leverage information and knowledge for more informed and effective decision-making that supports mission-driven strategic goals and technology investments.

It is increasingly rare to find business and technical knowledge in a single person. However, the founder of V3Main has relevant experience in both areas. Hence, he formed V3Main to best leverage the business and technical knowledge to enable clients to grow their businesses tactically and strategically and to remain competitive with the constant change in modern

Artificial Intelligence (AI) Solutions for Public Sector Entities

technology. The company started providing services to commercial clients related to the financial industry and expanded its services over the years to Oil and Gas, Healthcare, and Retail. In addition, V3Main has recently started providing services to Federal, State, and local government agencies.

Our endeavors, past and present, involve: Project/Program Management; Dynamic custom web applications; IT Managed Services; Cloud Services; User-friendly interfaces; Enterprise integration; Systems Development Life Cycle (SDLC); Scalable applications to integrate data with different systems through both functionality as well as infrastructure; Performance and up-time improvement; Cybersecurity; Custom security; Reporting KPIs (Key Performance Indicators), Big Data analytics and reporting; Open Source Technologies; MDM/MDS/BI/reporting; Backlog item tracking; Enterprise architecture;

Our success is largely due to working side by side with our customers to identify problems before investing resources and time to implement a solution. Additionally, deliberate conversations with the end-users as well as the developers and managers of systems are crucial to understanding how to implement a well-received solution that will adapt to and support an organization's greatest strengths.

We experienced in delivering the below projects:

- Implement NIST Cybersecurity Framework Compliance Protect, Detect, Respond and Recover from Cybersecurity related incidents. Incident Response Planning, Threat Analysis, vulnerability management.
- Develop E-Commerce Website using .Net, Entity Framework, Content Management, Deployment, SEO, Analytics and hosting the applications under Private and public cloud infrastructure.
- Currently, working on building new tools for V3Main using latest technologies, C++, Java and C#, Python, AngularJS, ReactJs, ReactNative, Web API, RESTfull APIs, Microservices, and Cloud Native. Design backend database(s) using SQL Azure, SQL Server, MySQL, MongoDB, creating stored procedures and complex queries. Integration of Social Media and Career websites
- Deploy and configure the applications under cloud infrastructure using Docker, Kubernetes containers.
- Develop custom applications using agile project management methodologies like Scrum, Kanban and utilized the agile project management tools like Jira, Confluence and TFS
- Maintain backlog items under TFS and Visual Studio Online VSO as a backlog board. generate reports in TFS and sync the work items.
- Manage multiple backlogs for a single team.
- Work with Product Owners and Portfolio Owners to define the backlogs, project planning and progress reporting.
- Maintain the Source code using Bitbucket, Github, Svn, Perforce and TFS
- Build the development infrastructure using private and public cloud infrastructure
- Implement the enterprise data security solution using Vormetric Data Security Manager. The Vormetric Data Security Manager centralizes policy control and key management for data-at-

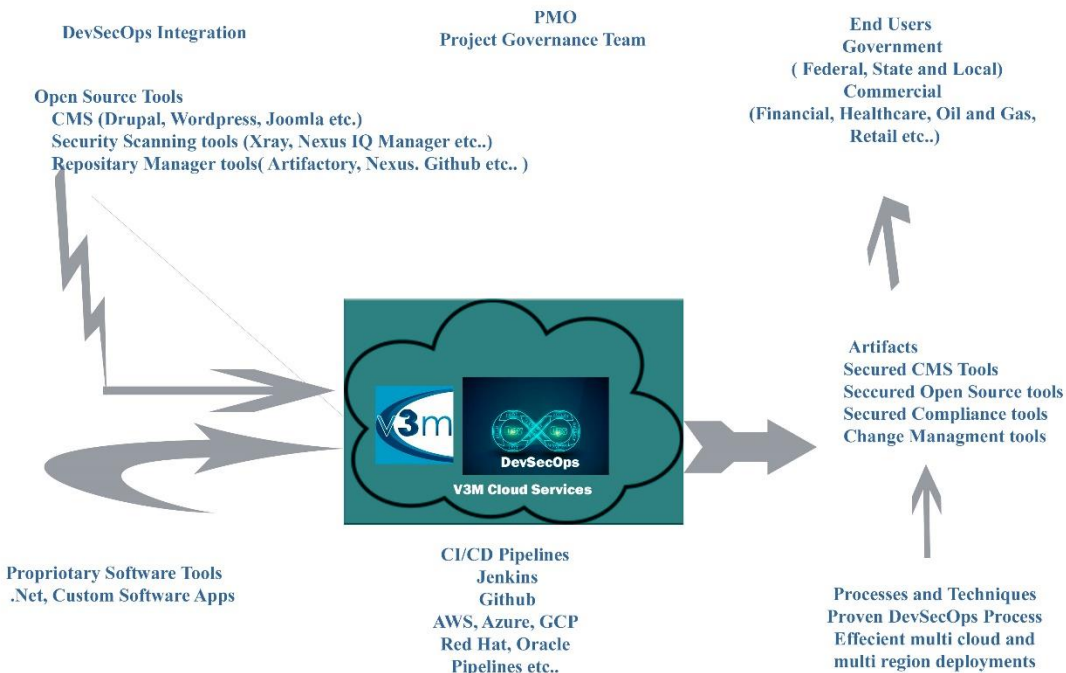
Artificial Intelligence (AI) Solutions for Public Sector Entities

rest-encryption, privileged user access control and security intelligence across an organization.

- Architecture and development of new SharePoint Websites using Office 365 Online and Exchange email Migration to Office 365. Extract email content through exchange web Services and save the content under SharePoint Web sites.
- Applications migration to new infrastructure with latest Cloud Virtualization technologies.
- Application deployment under IaaS, PaaS and SaaS environments (Azure, Oracle, Google Cloud, Openshift and AWS)
- DevOps Integration With Azure DevOps , Jenkins
- Big Data Analyssis using Apache Spark, Apache Hadoop, Apache Kafka
- Build external website to promote V3Main Services
- Deliver quality services by exceeding customer expectations. Automate and execute the client's business processes, deliver projects at lower cost with higher quality in a timely manner.
- Actively engaged the clients to acquire new opportunities while improving the internal business processes.

V3Main is partnered with AWS, Microsoft Azure, GCP, Oracle, and IBM to provide cloud-based services.

Cybersecurity and DevSecOps



V3Main Technologies**RFP-2025-018****www.v3mainglobal.com****Artificial Intelligence (AI) Solutions for Public Sector Entities**

We use the different Cybersecurity tools listed below to monitor network infrastructure and applications. Application software security scanning tools Nexus repository Manager, IQ Server, JFrog Artifactory, Xray, Veeam, Rubrik, and Penetration testing tools like Nexpose and Metasploit, Vormetric Data Security Manager, DELL EMC vSphere Optimization.

V3Main Software Development integrated with DevSecOps. V3Main Provides IT Managed Services focusing on Cybersecurity, Custom Software Development and Cloud Computing services. As part of our services, we do constant R&D related to the latest technologies and techniques to provide the best possible solutions to our clients. Our Big Data and Artificial Intelligence solutions leverages HPC, edge computing, 5G Network, cloud-native applications, backup & recovery solutions enables us to perform research on Climate Resilience solutions, build effective dashboards to provide up to date weather information, resources, supply chain alternatives in case of DR situations like Hurricane, Severe weather and tornados etc.

We have past performance performing similar tasks to manage the IT infrastructure, Cybersecurity services, Application Development, Mobile App development for end clients (Texas Comptroller of Public Accounts, City of Houston, General Dynamics, ASRC Federal, US Navy, Barclays, First Services Credit Union, Houston Calligraphy Guild, Davita, MattressFirm, eCardio, and HESS Corporation).

V3Main is an 8(a) certified, disadvantaged business enterprise. Many of our teaming partners are small businesses, women-owned, SDVOSB, HUBZone. Some of them have TS facility clearances along with TS personnel. Additionally, our team has ISO and CMMI level certifications.

We partnered with Parabola9 (“P9”) to provide AI Related Services using CyberPod COTS product especially designed for Gen AI related to Cybersecurity.

Together, V3Main and P9 can fulfill the overall Gen AI Services to Texas Share agencies.

6.2 Texas Comptroller of Public Accounts**Project title:** Enterprise Architectural Services**Description of the project:**

Enterprise IT Architectural Services including agile project management ,Infrastructure, Integration, cloud native applications development using .Net core, ESRI, and OpenShift.

Contract number: State of TX - Department of Information Resources (Enterprise Architect 2)
Scope:

- Analyze and research architecture patterns and implement software modifications keeping CPA's architecture vision and strategy in mind
- Analyzes requirements and specifications, develops, architects/designs, and coordinates the implementation of .Net applications and REST services with SQL Server back end.
- As part of the application development team, takes lead to solve technical challenges with industry best practices.

APPENDIX A.1
Pricing for TXShare Cooperative Purchase Program Participants

Category 1 - V3Main Technologies Pricing Details			
<div>Notes</div> <div>The pricing provided includes: •Solution design and documentation, including a comprehensive architecture tailored to the customer's requirements. •CyberPod AI implementation and customization as per the defined scope agreed upon with the customer. •Artificial intelligence advisory consulting services to guide the project and ensure optimal implementation. •Annual product support covering bug fixes and security updates for a period of one year, as per renewal cycle.</div>			
Description	Add additional description if necessary:	%Discount	Notes/ Comments
1. Software Licensing and Subscription Costs: Provide the cost breakdown for software licenses, subscriptions, or any other software-related fees.	Single Instance Deployment (On Premise)	5%	Year renewal price, post contract period price will be hiked by 12% per renewal.
2. Implementation and Customization Costs: Outline the costs related to the implementation of the AI solution, including setup, integration with existing systems, customization, and deployment.	AI Agents or Autopilots will be part of PS services		Unit price per hour as part of professional services.
3. Training and Support Costs: Include costs for training government staff, technical support, and customer service, both during and after implementation.	Part of post deployment handover	5%	Three working days workshop will be conducted.
4. Ongoing Maintenance and Updates: Provide costs for ongoing software maintenance, updates, and any regular services required to keep the AI system running smoothly.	Quarterly On-site visiting health check and maintenance support	5%	Annual Maintenance Optional
5. Optional Add-Ons or Features: List any additional features or services available that are not included in the core proposal but can be added at an additional cost.			
6. Total Cost of Ownership (TCO): Summarize the Total Cost of Ownership (TCO), which includes all costs over a defined period (e.g., 3 years or 5 years). This should reflect software, implementation, support, maintenance, and optional add-ons.		1 Year 10% 3 Year 20% 5 Year 30%	Additional Discount - 1 Year 10%, 3 Year 20%, 5 Year 30%
7. Additional Costs (if applicable): List any additional costs not covered in the above sections that are relevant to the proposal, such as travel costs, setup fees, or other miscellaneous charges.			Installation & Setup fee on-time cost
Category 2 - Ancillary Goods and/or Services			
Describe Below: Job Title	Job Function	%Discount	Notes/ Comments
ATO Implementation Program Manager	ATO - Implementation & Ongoing Maintenance	12%	
Chief Information Security Officer / SME	ATO - Implementation & Ongoing Maintenance	12%	
Chief Information Security Auditor	Audit Management	12%	
Data Security Specialist	Cloud Native Backup and Recovery Implementation Services	15%	
Computer Security Systems Specialist	CMMC, ISO, and SOC2 Audits	12%	
Cyber-Security Analyst/ Engineer	CMMC, ISO, and SOC2 Audits	12%	
Chief Information Officer (CIO)	Cybersecurity Implementation Support	15%	
Chief Information Security Officer (CISO)	Cybersecurity Implementation Support	15%	
Incident Response (IR)	Cybersecurity Implementation Support	15%	
Information System Owner (SO)	Cybersecurity Implementation Support	15%	
Information Systems Security Officer (ISSO)	Cybersecurity Implementation Support	15%	
Junior Information Security Analyst (Cybersecurity Analyst)	Cybersecurity Implementation Support	15%	
Junior Information Systems Security Officer (ISSO)	Cybersecurity Implementation Support	15%	
Mid Level Information Security Analyst (Cybersecurity Analyst)	Cybersecurity Implementation Support	15%	
Mid Level Information Systems Security Officer (ISSO)	Cybersecurity Implementation Support	15%	
Program Manager	Cybersecurity Implementation Support	15%	
Security Control Access or (SCA)	Cybersecurity Implementation Support	15%	
Senior Computer Systems Analyst (Sr. DevSecOps Engineer)	Cybersecurity Implementation Support	15%	
Senior Information Security Analyst (Cybersecurity Analyst)	Cybersecurity Implementation Support	15%	
Senior Information Systems Security Officer (ISSO)	Cybersecurity Implementation Support	15%	
Data Center Facilities Project Manager(s)	Data Center Implementation Services	15%	
SME/Computer Systems Engineer Architect	Data center Services (Colocation, IaaS) Implementation Support	15%	
Disaster Recovery Specialist	Disaster Recovery Services	15%	
Disaster Recovery Specialist	Disaster Recovery Services	15%	
Senior Database Architect	Enterprise Architectural Services	15%	
SME/Computer Systems Engineer Architect	Enterprise Architectural Services	15%	
Data Scientist	Enterprise Architecture Services	15%	
Configuration Management Specialist	Identity and Access Management Services (IAM) Implementation	12%	
Journeyman Business Intelligence Analyst	Implementation Support	12%	
Journeyman Computer User Support Specialist	Implementation Support	15%	
Journeyman Software Quality Assurance Engineer and Tester	Implementation Support	15%	
Junior Software Quality Assurance Engineer and Tester	Implementation Support	15%	
Senior Database Administrator	Implementation Support	12%	
Senior Software Quality Assurance Engineer and Tester	Implementation Support	15%	
Senior Technical Writer	Implementation Support	15%	
Senior Training and Specialist	Implementation Support	15%	
Cyber-Security Analyst/ Engineer	Key Management Service (PKI)	15%	
Configuration Management Specialist	Network Management Services	15%	
Senior Network and Computer Systems Administrator	Network Management Services	15%	
Senior Network and Computer Systems Administrator	Network Management Services	15%	
Security Engineer – Penetration Testing	Pen Testing	15%	
Journeyman Information Technology Project Manager	Project Management	12%	
Program Manager	Project Management	12%	
Project Manager	Project Management	12%	
Senior Information Technology Project Manager	Project Management	12%	
Journeyman Information Security Analyst	Security Implementation Services	12%	
Journeyman Software Quality Assurance Engineer and Tester	Security Implementation Services	20%	
Senior Computer and Information Systems Manager	Security Implementation Services	20%	
Senior Computer Systems Analyst (Sr. DevSecOps Engineer)	Security Implementation Services	20%	
Senior Computer Systems Engineer Architect	Security Implementation Services	20%	
Senior Database Administrator	Security Implementation Services	15%	
SME/Computer Systems Analyst	Security Implementation Services	15%	
SME/Computer Systems Engineer Architect	Security Implementation Services	15%	
Senior Computer Systems Analysts (Sr. Engineer)	Zero Trust Network Architecture (ZTA) Implementation	15%	
Senior Information Security Analyst (Cybersecurity Analyst)	Zero Trust Network Architecture (ZTA) Implementation	12%	

The Contractor shall ensure that any ancillary goods or services provided in connection with AI Solutions are consistent with the technical and operational standards outlined in this agreement and relevant to AI Solutions.

EXHIBIT 3: SERVICE DESIGNATION AREAS

Texas Service Area Designation or Identification			
Proposing Firm Name:	V3Main Technologies, Inc.		
Notes:	Indicate in the appropriate box whether you are proposing to service the entire state of Texas		
	Will service the entire state of Texas	Will not service the entire state of Texas	
	<input checked="checked" type="checkbox"/>	<input type="checkbox"/>	
	If you are not proposing to service the entire state of Texas, designate on the form below the regions that you are proposing to provide goods and/or services to. By designating a region or regions, you are certifying that you are willing and able to provide the proposed goods and services.		
Item	Region	Metropolitan Statistical Areas	Designated Service Area
1.	North Central Texas	16 counties in the Dallas-Fort Worth Metropolitan area	
2.	High Plains	Amarillo Lubbock	
3.	Northwest	Abilene Wichita Falls	
4.	Upper East	Longview Texarkana, TX-AR Metro Area Tyler	
5.	Southeast	Beaumont-Port Arthur	
6.	Gulf Coast	Houston-The Woodlands-Sugar Land	
7.	Central Texas	College Station-Bryan Killeen-Temple Waco	
8.	Capital Texas	Austin-Round Rock	
9.	Alamo	San Antonio-New Braunfels Victoria	
10.	South Texas	Brownsville-Harlingen Corpus Christi Laredo McAllen-Edinburg-Mission	
11.	West Texas	Midland Odessa San Angelo	
12.	Upper Rio Grande	El Paso	

(Exhibit 3 continued on next page)

(Exhibit 3 continued)

Nationwide Service Area Designation or Identification Form			
Proposing Firm Name:	V3Main Technologies, Inc.		
Notes:	<p>Indicate in the appropriate box whether you are proposing to provide service to all Fifty (50) States.</p> <p>Will service all fifty (50) states <input checked="checked" type="checkbox"/> Will not service fifty (50) states <input type="checkbox"/></p> <p>If you are not proposing to service to all fifty (50) states, then designate on the form below the states that you will provide service to. By designating a state or states, you are certifying that you are willing and able to provide the proposed goods and services in those states.</p> <p>If you are only proposing to service a specific region, metropolitan statistical area (MSA), or City in a State, then indicate as such in the appropriate column box.</p>		
Item	State	Region/MSA/City (write "ALL" if proposing to service entire state)	Designated as a Service Area
1.	Alabama		
2.	Alaska		
3.	Arizona		
4.	Arkansas		
5.	California		
6.	Colorado		
7.	Connecticut		
8.	Delaware		
9.	Florida		
10.	Georgia		
11.	Hawaii		
12.	Idaho		
13.	Illinois		
14.	Indiana		
15.	Iowa		
16.	Kansas		
17.	Kentucky		
18.	Louisiana		
19.	Maine		
20.	Maryland		

21.	Massachusetts		
22.	Michigan		
23.	Minnesota		
24.	Mississippi		
25.	Missouri		
26.	Montana		
27.	Nebraska		
28.	Nevada		
29.	New Hampshire		
30.	New Jersey		
31.	New Mexico		
32.	New York		
33.	North Carolina		
34.	North Dakota		
35.	Ohio		
36.	Oregon		
37.	Oklahoma		
38.	Pennsylvania		
39.	Rhode Island		
40.	South Carolina		
41.	South Dakota		
42.	Tennessee		
43.	Texas		
44.	Utah		
45.	Vermont		
46.	Virginia		
47.	Washington		
48.	West Virginia		
49.	Wisconsin		
50.	Wyoming		

End of Exhibit 3

APPENDIX B

NCTCOG FEDERAL AND STATE OF TEXAS REQUIRED PROCUREMENT PROVISIONS
The following provisions are mandated by Federal and/or State of Texas law. Failure to certify to the following will result in disqualification of consideration for contract. Entities or agencies that are not able to comply with the following will be ineligible for consideration of contract award.

REQUIRED 2 CFR 200 CLAUSES

Uniform Administrative Requirements, Cost Principles & Audit Requirements for Federal Awards (Contractor)

1. **Equal Employment Opportunity.** CONTRACTOR shall not discriminate against any employee or applicant for employment because of race, religion, color, sex, sexual orientation, gender identity, or national origin. CONTRACTOR shall take affirmative actions to ensure that applicants are employed, and that employees are treated, during their employment, without regard to their race, religion, color, sex, sexual orientation, gender identity, or national origin. Such actions shall include, but not be limited to, the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.
2. **Davis-Bacon Act.** CONTRACTOR agrees to comply with all applicable provisions of 40 USC § 3141 – 3148.
3. **Contract Work Hours and Safety Standards.** CONTRACTOR agrees to comply with all applicable provisions of 40 USC § 3701 – 3708 to the extent this agreement indicates any employment of mechanics or laborers.
4. **Rights to Invention Made Under Contract or Agreement.** CONTRACTOR agrees to comply with all applicable provisions of 37 CFR Part 401.
5. **Clean Air Act, Federal Water Pollution Control Act, and Energy Policy Conservation Act.** CONTRACTOR agrees to comply with all applicable provisions of the Clean Air Act under 42 USC § 7401 – 7671, the Energy Federal Water Pollution Control Act 33 USC § 1251 – 1387, and the Energy Policy Conservation Act under 42 USC § 6201.
6. **Debarment/Suspension.** CONTRACTOR is prohibited from making any award or permitting any award at any tier to any party which is debarred or suspended or otherwise excluded from or ineligible for participation in federal assistance programs under Executive Order 12549, Debarment and Suspension. CONTRACTOR and its subcontractors shall comply with the special provision “Certification Requirements for Recipients of Grants and Cooperative Agreements Regarding Debarments and Suspensions”.
7. **Restrictions on Lobbying.** CONTRACTOR of these funds is prohibited from using monies for lobbying purposes; CONTRACTOR shall comply with the special provision “Restrictions on Lobbying”. CONTRACTOR shall include a statement of compliance with the Lobbying Certification and Disclosure of Lobbying Activities in applicable procurement solicitations. Lobbying Certification and Disclosure of Lobbying Activities shall be completed by subcontractors and included in subcontractor contracts, as applicable.
8. **Procurement of Recovered Materials.** CONTRACTOR agrees to comply with all applicable provisions of 2 CFR §200.322.
9. **Anti-Israeli Boycott.** By accepting this work order, CONTRACTOR hereby certifies the following:
 1. CONTRACTOR’s Company does not boycott Israel; and
 2. CONTRACTOR’s Company will not boycott Israel during the term of the contract.

The following definitions apply to this statute:

- (1) "Boycott Israel" means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli- controlled territory, but does not include an action made for ordinary business purposes; and
- (2) "Company" means an organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, including wholly owned subsidiary, majority-owned subsidiary, parent company, or affiliate of those entities or business associations that exists to make a profit.

10. Domestic Preference for Procurements

As appropriate and to the extent consistent with law, the CONTRACTOR should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). Consistent with §200.322, the following items shall be defined as: “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. “Manufactured products” means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

11. Trafficking in Persons

Contractor agrees to comply with all applicable provisions of 2 CFR §175.15. NCTCOG, the Contractor, and its subcontractors are prohibited from (i) engaging in severe forms of trafficking in persons during the period of time that the award is in effect; (ii) procure a commercial sex act during the period of time that the award is in effect; (iii) used force labor in the performance of the award or subawards under the award. The Federal award agency may unilaterally terminate the award, without penalty, if the Contractor (i) is determined to have violated an applicable prohibition; (ii) has an employee who is determined by the agency officially authorized to terminate the award to have violated an applicable prohibition of this award term. NCTCOG must notify the Federal award agency immediately if any information received from the Contractor indicates a violation of the applicable prohibitions.

Check one of the following:

- ☒ The Contractor or Subrecipient hereby certifies that it **does** comply with the requirements of 2 CFR 200 as stipulated above and required by the NCTCOG.

-OR-

- ☐ The Contractor or Subrecipient hereby certifies that it **cannot** comply with the requirements of 2 CFR 200 as stipulated above and required by the NCTCOG.



Signature of Authorized Person
Venkat Maddikayala, President and CEO

Name of Authorized Person
V3MAIN TECHNOLOGIES, INC.

Name of Company
05/08/2025

Date

APPENDIX C RESTRICTIONS ON LOBBYING

Section 319 of Public Law 101-121 prohibits recipients of federal contracts, grants, and loans exceeding \$100,000 at any tier under a federal contract from using appropriated funds for lobbying the Executive or Legislative Branches of the federal government in connection with a specific contract, grant, or loan. Section 319 also requires each person who requests or receives a federal contract or grant in excess of \$100,000 to disclose lobbying.

No appropriated funds may be expended by the recipient of a federal contract, loan, or cooperative agreement to pay any person for influencing or attempting to influence an officer or employee of any federal executive department or agency as well as any independent regulatory commission or government corporation, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered federal actions: the awarding of any federal contract, the making of any federal grant, the making of any federal loan the entering into of any cooperative agreement and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

As a recipient of a federal grant exceeding \$100,000, NCTCOG requires its subcontractors of that grant to file a certification, set forth in Appendix B.1, that neither the agency nor its employees have made, or will make, any payment prohibited by the preceding paragraph.

Subcontractors are also required to file with NCTCOG a disclosure form, set forth in Appendix B.2, if the subcontractor or its employees have made or have agreed to make any payment using nonappropriated funds (to include profits from any federal action), which would be prohibited if paid for with appropriated funds.

**LOBBYING CERTIFICATION
FOR CONTRACTS, GRANTS, LOANS, AND COOPERATIVE AGREEMENTS**

The undersigned certifies to the best of his or her knowledge and belief, that:

- (1) No federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension continuation, renewal amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form - LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, US Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.



Signature

President and CEO

Title

V3MAIN TECHNOLOGIES, INC.

Agency

05/08/2025

Date

APPENDIX D
PROHIBITED TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR
EQUIPMENT CERTIFICATION

This Contract is subject to the Public Law 115-232, Section 889, and 2 Code of Federal Regulations (CFR) Part 200, including §200.216 and §200.471, for prohibition on certain telecommunications and video surveillance or equipment.

Public Law 115-232, Section 889, identifies that restricted telecommunications and video surveillance equipment or services (e.g. phones, internet, video surveillance, cloud servers) include the following:

- A) Telecommunications equipment that is produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliates of such entities).
- B) Video surveillance and telecommunications equipment produced by Hytera Communications Corporations, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliates of such entities).
- C) Telecommunications or video surveillance services used by such entities or using such equipment.
- D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, Director of the National Intelligence, or the Director of the Federal Bureau of Investigation reasonably believes to be an entity owned or controlled by the government of a covered foreign country.

The entity identified below, through its authorized representative, hereby certifies that no funds under this Contract will be obligated or expended to procure or obtain telecommunication or video surveillance services or equipment or systems that use covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as part of any system prohibited by 2 CFR §200.216 and §200.471, or applicable provisions in Public Law 115-232 Section 889.

Check one of the following:

☒ The Contractor or Subrecipient hereby certifies that it **does** comply with the requirements of 2 CFR 200 as stipulated above and required by the NCTCOG.

-OR-

☐ The Contractor or Subrecipient hereby certifies that it **cannot** comply with the requirements of 2 CFR 200 as stipulated above and required by the NCTCOG.



 Signature of Authorized Person

Venkat Maddikayala, President and CEO

 Name of Authorized Person

V3MAIN TECHNOLOGIES, INC.

 Name of Company

05/08/2025

 Date

**DISCRIMINATION AGAINST FIREARMS ENTITIES OR FIREARMS TRADE
ASSOCIATIONS**

This contract is subject to the Texas Local Government Code chapter 2274, Subtitle F, Title 10, prohibiting contracts with companies who discriminate against firearm and ammunition industries.

TLGC chapter 2274, Subtitle F, Title 10, identifies that “discrimination against a firearm entity or firearm trade association” includes the following:

- A) means, with respect to the entity or association, to:
 - I. refuse to engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; and
 - II. refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or
 - III. terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association.
- B) An exception to this provision excludes the following:
 - I. contracts with a sole-source provider; or
 - II. the government entity does not receive bids from companies who can provide written verification.

The entity identified below, through its authorized representative, hereby certifies that they have no practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association; and that they will not discriminate during the term of the contract against a firearm entity or firearm trade association as prohibited by Chapter 2274, Subtitle F, Title 10 of the Texas Local Government Code.

Check one of the following:

☒ The Contractor or Subrecipient hereby certifies that it does comply with the requirements of Chapter 2274, Subtitle F, Title 10.

-OR-

☐ The Contractor or Subrecipient hereby certifies that it cannot comply with the requirements of Chapter 2274, Subtitle F, Title 10.



Signature of Authorized Person

Venkat Maddikayala, President and CEO

Name of Authorized Person

V3MAIN TECHNOLOGIES, INC.

Name of Company

05/08/2025

Date

BOYCOTTING OF CERTAIN ENERGY COMPANIES

This contract is subject to the Texas Local Government Code chapter 809, Subtitle A, Title 8, prohibiting contracts with companies who boycott certain energy companies.

TLGC chapter Code chapter 809, Subtitle A, Title 8, identifies that “boycott energy company” means, without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company:

- I. engages in the exploration, production, utilization, transportation, sale, or manufacturing of fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law; and
- II. does business with a company described by paragraph (I).

The entity identified below, through its authorized representative, hereby certifies that they do not boycott energy companies, and that they will not boycott energy companies during the term of the contract as prohibited by Chapter 809, Subtitle A, Title 8 of the Texas Local Government Code.

Check one of the following:

- ☒ The Contractor or Subrecipient hereby certifies that it **does** comply with the requirements of Chapter 809, Subtitle A, Title 8.

-OR-

- ☐ The Contractor or Subrecipient hereby certifies that it **cannot** comply with the requirements of Chapter 809, Subtitle A, Title 8.



Signature of Authorized Person

Venkat Maddikayala, President and CEO

Name of Authorized Person

V3MAIN TECHNOLOGIES, INC.

Name of Company

05/08/2025

Date

APPENDIX E
DEBARMENT CERTIFICATION

Venkat Maddikayala _____ being duly
(Name of certifying official)
sworn or under penalty of perjury under the laws of the United States, certifies that neither

Parabola9 _____, nor its principals
(Name of lower tier participant)
are presently:

- debarred, suspended, proposed for debarment,
- declared ineligible,
- or voluntarily excluded from participation in this transaction by any federal department or agency

Where the above identified lower tier participant is unable to certify to any of the above statements in this certification, such prospective participant shall indicate below to whom the exception applies, the initiating agency, and dates of action.

Exceptions will not necessarily result in denial of award but will be considered in determining contractor responsibility. Providing false information may result in criminal prosecution or administrative sanctions.

EXCEPTIONS:



Signature of Certifying Official

Title President and CEO

Date of Certification 05/08/2025

Form 1734
Rev.10-91
TPFS