

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

Def-Logix, Inc. ("Contractor")
3463 Magic Drive, Ste 220
Austin, TX 78229

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 Pricing for items in Appendix A represent the maximum cost for each item offered by the Contractor. Contractor and Participating Entity may mutually agree to a lower cost 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:

Def-Logix, Inc.

Attn: Carolina Frias-Costa

3463 Magic Drive, Ste. 220

San Antonio, TX 78229

Phone: 210-624-7915

Email: cfcosta@def-logix.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).
- l. 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.

Def-Logix, Inc.

North Central Texas Council of Governments



01 May 2025

Signature

Date

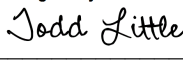
Carolina Frias-Costa

Printed Name

Director of Contracts & Capture

Title

Signed by:



6/1/2025

Date

Signature

232D24222B0842B...

Todd Little

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.



Our organization is driven by a mission to advance technology and innovation in service to our government and commercial customers, empowering them to meet critical cybersecurity challenges with confidence. Guided by our core values of innovation, integrity, teamwork, and excellence, we are dedicated to developing cutting-edge technologies and solutions that strengthen the cybersecurity posture, increase situational awareness, and provide robust defenses against malicious cyber-attacks. We are deeply committed to fostering a collaborative and inspiring environment for our employees, where teamwork, creativity, and innovation thrive. Recognizing the importance of a skilled workforce, our CyberOps Training Academy plays a vital role in bridging the gap between education and careers in cybersecurity. By equipping students with in-demand skills and hands-on experience, we contribute to building a strong and resilient cyber workforce prepared to address evolving threats.

Through our unwavering dedication to excellence and innovation, we continue to push the boundaries of what is possible, delivering impactful solutions that protect, empower, and inspire.

3.4 Significant Requirements Not Met

Def-Logix is confident in meeting all significant requirements outlined in the Scope of Work.

Statement of Limitations: At this time, there are no significant requirements from the Scope of Work that Def-Logix is unable to meet. Should any constraints arise during the project lifecycle, they will be promptly communicated with proposed solutions.

4 Technical Proposal

4.1 Project Deliverables

Def-Logix is dedicated to delivering innovative and customized solutions that align with the specific deliverables outlined in the project scope. Our approach is designed to support public sector entities by addressing their unique challenges and requirements, ensuring efficient, effective, and sustainable outcomes. Below, we detail how our proposed solution will help achieve each deliverable while meeting the objectives of these entities. Below is a detailed breakdown of how our solution aligns with and fulfills the technical objectives: Information Technology and Cybersecurity (IT).

4.1.1 Information Technology and Cybersecurity (IT)

Def-Logix has already developed Crimson Raven, an advanced AI solution designed to reduce the workload of IT personnel by automating repetitive tasks, optimizing processes, enhancing cybersecurity, and improving service management. We will modify Crimson Raven to tailor it to each city's unique needs and integrate it with existing city infrastructure, ensuring scalability and long-lasting impact. By automating routine functions, streamlining workflows, and strengthening cybersecurity measures, these solutions enable IT teams to operate more efficiently and focus on strategic initiatives.

By integrating Crimson Raven and other AI technologies, we propose a tailored solution to meet the objective of alleviating the workload of IT personnel while improving public services, optimizing data usage, and increasing citizen engagement. The following table demonstrates how Crimson Raven, along with AI-driven capabilities, can enhance key aspects of information technology and cybersecurity within the public sector, driving operational efficiency and strengthening security protocols.

Table 2 - AI-driven IT and Cybersecurity Enhancements for the Public Sector.

Area	AI Assistance	Benefits
Automating Help Desk Support	AI Chatbots and Virtual Assistants	AI-driven chatbots address common issues (e.g., password resets, and software installations), significantly reducing support ticket volume and freeing up IT resources for more complex tasks.
	Ticket Routing and Prioritization	AI intelligently categorizes, prioritizes, and routes tickets based on their complexity and urgency, accelerating response times and improving issue resolution.



Streamlining IT Processes	Automated Task Management	Crimson Raven automates tasks related to red team operations, such as the execution of TTPs, incident response protocols, and security checks, as well as routine tasks like software updates, patch management, and system backups, ensuring timely completion and reducing manual oversight.
	Predictive Maintenance	By monitoring system logs and threat intelligence feeds, Crimson Raven predicts potential cybersecurity weaknesses and offers suggestions for timely interventions, reducing downtime and enhancing operational efficiency.
Creating Documentation	Automated Knowledge Base Creation	Crimson Raven generates and updates real-time knowledge base articles for operators by analyzing red team activity, incident logs, service tickets, and MITRE ATT&CK framework data, ensuring easy access to up-to-date, actionable technical information.
	Contextual Documentation Generation	Crimson Raven creates tailored, relevant documentation for red team operators based on real-time engagements, incidents, and system configurations, ensuring accuracy, knowledge retention, and updates aligned with the latest activities and TTP.
Cybersecurity Threat Detection	Real-Time Threat Monitoring	Crimson Raven analyzes network traffic and system data in real-time to detect potential cybersecurity threats, enabling faster and more accurate identification of threats.
	Behavioral Analysis and Anomaly Detection	By tracking and analyzing patterns in red team operations and network behaviors, Crimson Raven identifies unusual activities or anomalies, potentially flagging malicious actions before escalation.
	Automated Incident Response	Crimson Raven triggers automated responses, such as isolating compromised systems and blocking malicious IPs, based on predefined TTPs, ensuring swift reactions to cybersecurity incidents.
Proactive Auditing and Cyber Defense	Continuous Security Auditing	Crimson Raven continuously scans cybersecurity infrastructure for vulnerabilities or compliance gaps, offering proactive solutions before threats materialize.
	Predictive Cyber Defense	Crimson Raven analyzes historical attack patterns and suggests predictive defense strategies to mitigate emerging threats, improving long-term security posture.
	Compliance Automation	AI automates the auditing process for regulatory compliance (e.g., GDPR, HIPAA), ensuring adherence to standards and simplifying reporting.

The central challenge in enhancing public services is to improve service delivery, optimize data usage, and foster greater citizen engagement. AI solutions, such as Crimson Raven, are well-suited to address these challenges in the following ways:

- **Improve Public Services:** AI-driven automation, predictive analytics, and real-time decision-making can streamline government operations, optimize service delivery, and enhance public sector efficiency.
- **Optimize Data Usage:** AI can process vast datasets more efficiently, providing valuable insights for decision-makers and enabling actionable data to be leveraged for public service improvement.
- **Increase Citizen Engagement:** By leveraging conversational AI, government agencies can provide better interaction with citizens, automate responses to queries, and offer personalized, timely services.

4.2 Technical Approach

Def-Logix is committed to delivering a scalable, advanced AI solution through Crimson Raven, specifically tailored to meet the unique requirements of government systems. Our approach integrates robust design and development methodologies with seamless system integration, prioritizing user-friendliness and accessibility. By combining the capabilities of our AI platform with the specific needs of public services,



we focus on data processing, automation, citizen engagement, and predictive analytics to optimize service delivery and enhance interactions with the public.

Our technical approach is centered around modifying Crimson Raven to address the unique needs of each city. We will tailor the platform to integrate seamlessly with existing city systems, ensuring scalability, ease of adoption, and long-term sustainability. By customizing the AI-driven capabilities of Crimson Raven, we aim to reduce the workload of IT personnel, optimize data usage, automate repetitive tasks, and enhance service management. This approach not only enhances the effectiveness of public sector operations but also ensures a continuous, adaptive solution capable of evolving alongside future technological advancements.

4.2.1 Methodologies for design and development

Def-Logix’s design and development methodologies prioritize innovation, scalability, and user-centric solutions. With Crimson Raven’s end-to-end AI-driven optimization, the platform will seamlessly integrate data, leverage predictive analytics, and automate routine tasks, ensuring a proactive and efficient approach to IT management and service delivery. By focusing on a tailored solution that aligns with each city’s unique needs, we will deliver measurable improvements across public services, cybersecurity, and citizen engagement. Key activities include:

Table 3 - Def-Logix Design and Development Methodologies

Phases	Activities	Outcomes
Data Collection and Integration	<ul style="list-style-type: none">Gather data from government systems, citizen feedback, and service requests into a unified system.Utilize Crimson Raven's AI capabilities to process and convert data into actionable insights.	Enhanced decision-making and improved service outcomes through centralized data analysis.
Integration Planning	<ul style="list-style-type: none">Map integration points with existing systems.Design APIs and middleware for seamless connectivity.	Compatibility across diverse systems and real-time data exchange.
AI-Driven Automation	<ul style="list-style-type: none">Automate routine tasks such as processing permits and renewals using AI-powered chatbots.Route complex issues to human agents while prioritizing urgent cases.	Reduced workload for IT personnel and increased citizen satisfaction.
Predictive Analytics	<ul style="list-style-type: none">Leverage AI-driven predictive analytics to identify patterns and allocate resources effectively.	Improved operational efficiency and service reliability through proactive measures.
Testing & Validation	<ul style="list-style-type: none">Conduct extensive unit, system, and user acceptance testing.Ensure compliance with regulations like FISMA and TX-RAMP.	Reliable, secure, and compliant solution ready for deployment.

4.2.2 Integration strategies with existing government systems

Def-Logix will ensure a seamless transition to Crimson Raven by employing a combination of middleware, APIs, and predictive analytics, guaranteeing smooth integration with existing infrastructure. We will focus on leveraging open-source technologies to extend the platform's flexibility and adaptability, enabling efficient integration with a wide range of systems and tools. The approach outlined in Table 4 will provide a scalable and secure solution that is future-proof while maintaining compliance and operational integrity throughout the integration process.



Table 4 - Def-Logix Integration Strategy for Crimson Raven

Integration Strategy	Description	Benefits
API-Based Communication	<ul style="list-style-type: none">Implement RESTful APIs for data exchange between Crimson Raven and government systems.Enable real-time synchronization across departments.	Ensures consistent data access and operational efficiency.
Middleware for Legacy Systems	<ul style="list-style-type: none">Introduce middleware to bridge modern AI functionalities with legacy infrastructure.	Facilitates compatibility without requiring costly system overhauls.
Phased Deployment	<ul style="list-style-type: none">Deploy Crimson Raven in stages, starting with low-risk environments to refine processes and gather feedback.	Minimizes risk and ensures uninterrupted service delivery during integration.
Predictive Maintenance	<ul style="list-style-type: none">Use predictive analytics to monitor integration performance and preempt potential issues.	Avoids disruptions and maintains service quality.
Regulatory Alignment	<ul style="list-style-type: none">Embed compliance mechanisms (e.g., encryption, RBAC) during integration to meet local, state, and federal requirements.	Safeguards sensitive data and ensures regulatory compliance.

4.2.3 User-friendliness and accessibility considerations

Crimson Raven will prioritize user engagement and inclusivity, offering an intuitive experience for IT personnel, government employees, and citizens. Its conversational AI will facilitate natural, real-time interactions, boosting citizen trust and enhancing overall engagement with public services.

Table 5 - Crimson Raven User-Friendliness and Accessibility Considerations

Key Features	Description	Benefits
Intuitive Dashboards	Provide real-time visualizations of data trends and system performance.	Simplifies decision-making for IT personnel and government leaders.
Natural Language Interfaces	Enable citizens to engage through AI-powered chatbots embedded in websites, mobile apps, and kiosks.	Enhances citizen satisfaction with real-time, intuitive responses.
Customizable Interfaces	Allow personalization to meet the specific needs of different departments or user groups.	Improves adaptability and efficiency for diverse use cases.
Accessibility Compliance	Adhere to WCAG 2.1 and Section 508 standards with features like screen reader compatibility and keyboard navigation.	Ensures inclusivity for users with disabilities, promoting equitable access to services.
Feedback Integration	Continuously gather user feedback to refine features and enhance usability.	Drives user-centered improvements and long-term system relevance.

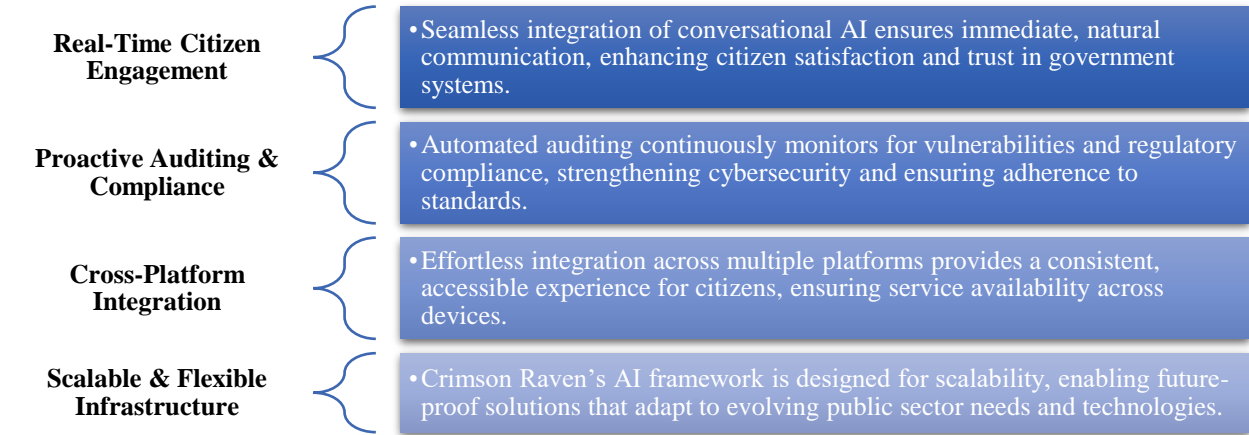


Figure 4 - Crimson Raven's AI-Driven Citizen Engagement Framework



Def-Logix's technical approach integrates Crimson Raven seamlessly into government systems while emphasizing data-driven decision-making, automation, and user-friendly design. By leveraging advanced AI capabilities, this approach not only reduces the workload for IT personnel but also transforms public service delivery, ensuring improved efficiency, security, and citizen satisfaction.

4.3 Technical Requirements

4.3.1 Challenge-Specific Functionality

We will tailor our AI solution, Crimson Raven, to meet the unique requirements of each entity, addressing specific challenges such as automating routine service processes, enhancing citizen engagement, and ensuring proactive cybersecurity. The platform will integrate predictive analytics, real-time data processing, and conversational AI to support functionalities such as AI-driven automation of services, compliance monitoring, and resource optimization. By continuously adapting to the needs of each organization, Crimson Raven will provide a customizable, efficient, and effective solution that improves both operational performance and citizen satisfaction.

4.3.2 Scalability

Crimson Raven is designed with scalability at its core, ensuring it can handle fluctuating data volumes and varying interaction levels without compromising performance. The solution leverages a cloud-based infrastructure that dynamically adjusts to meet growing demands, whether in terms of data processing, user interactions, or system integrations. As the needs of the entity evolve, Crimson Raven can seamlessly scale to accommodate increased workloads, making it a future-proof solution that supports long-term operational growth and ensures continuous service availability, even during peak periods.

4.3.3 Integration

Crimson Raven will be integrated with security frameworks such as Mobile Device Management (MDM), Identity and Access Management (IAM), Security Information and Event Management (SIEM), and other essential IT infrastructure components to ensure secure, scalable, and adaptable operations. To achieve seamless connectivity, we will expose web services to Crimson Raven, allowing it to interface with each system. The integration will be executed on a case-by-case basis, carefully considering the distinct requirements and configurations of each system. This customized approach guarantees that Crimson Raven integrates smoothly with the existing infrastructure, enhancing functionality while preserving security and optimal performance.

4.3.4 Real-Time Analytics

Crimson Raven's ability to log and track tokens across agents ensures secure and efficient access management, significantly enhancing system integrity and performance. By securely managing access tokens, the platform provides precise control over who can access specific resources and functionalities. This robust access control mechanism not only helps safeguard sensitive data but also optimizes performance by ensuring that only authorized users and agents interact with the system. This level of security and efficiency ensures that Crimson Raven operates smoothly, providing consistent and reliable service delivery across integrated government systems.

4.3.5 Data Security and Privacy

Def-Logix will ensure that Crimson Raven fully complies with relevant data security and privacy regulations, such as GDPR, HIPAA, and other local, state, and federal standards. Data security is a core aspect of the platform's design, which incorporates industry-leading encryption protocols, access control mechanisms, and secure data storage solutions to protect sensitive citizen data and prevent unauthorized access. Additionally, Crimson Raven will implement a proactive monitoring system that continuously scans for potential security vulnerabilities, allowing us to mitigate risks before they escalate into threats. By



strictly adhering to privacy regulations and employing robust cybersecurity practices, Crimson Raven will safeguard public service systems and ensure that citizens' personal information remains protected.

4.3.6 Natural Language Processing Capabilities

Crimson Raven incorporates advanced Natural Language Processing (NLP) capabilities, enabling the AI system to understand and respond to a wide range of citizen inquiries in a conversational, intuitive manner. This facilitates seamless interactions with users through chatbots and automated response systems. The NLP engine is designed to interpret various languages, dialects, and types of inquiries accurately, ensuring citizens from diverse backgrounds can easily engage with the system. Additionally, we are currently working on integrating voice-to-text functionality, further enhancing communication and allowing citizens to interact more naturally. By leveraging NLP, Crimson Raven will improve citizen engagement, delivering prompt, relevant responses related to public services, compliance, and other government functions, thus fostering a more positive citizen experience.

4.3.7 Accuracy

Crimson Raven is engineered to ensure a high level of accuracy in processing data and generating responses, which is critical for maintaining trust and effectiveness across all functionalities. Crimson Raven already utilizes advanced machine learning models, including natural language processing (NLP) and predictive analytics, to ensure that every interaction, decision, and output is grounded in accurate, real-time data. To measure and maintain accuracy, the solution follows a rigorous process throughout its lifecycle:

- 1. Data Validation:** Crimson Raven incorporates robust data validation protocols at every stage of data collection and integration, ensuring that input data from government systems, service requests, and citizen interactions is clean, consistent, and accurate before it is processed.
- 2. Continuous Model Training:** The platform's machine learning models are constantly retrained using the latest data, improving their predictive power and accuracy over time. By continuously learning from new inputs and real-world scenarios, the system adapts and fine-tunes its responses to ensure optimal accuracy.
- 3. Real-Time Monitoring and Feedback Loops:** Crimson Raven includes built-in mechanisms for real-time monitoring and feedback collection. Any inaccuracies detected in the system's output are automatically flagged, and corrective actions are taken immediately to rectify these issues. This is especially important for complex tasks such as AI-driven automation of services and conversational AI responses.
- 4. Performance Metrics and Accuracy Dashboards:** To measure and track accuracy, the system includes key performance indicators (KPIs) that monitor the precision of data processing and responses generated by the AI. These metrics are presented through interactive dashboards that allow administrators to track trends and identify potential accuracy issues, ensuring continuous improvement.
- 5. Regular Auditing and Quality Assurance:** Regular audits and quality assurance checks are built into the solution's lifecycle. These audits examine system performance, ensuring that all responses, automated processes, and data-driven decisions align with predefined accuracy standards. These checks help maintain high accuracy levels, even as new features or updates are implemented.
- 6. User Feedback and Adaptation:** Finally, Crimson Raven's interface allows end-users to provide feedback on the accuracy of AI-generated responses. This feedback is processed by the system and used to fine-tune the algorithms, ensuring that user interactions continuously improve over time.

Through this multi-layered approach, Crimson Raven guarantees a high level of accuracy in processing data and generating responses, continuously maintaining and enhancing the precision of the solution throughout its lifecycle.



4.3.8 Algorithm Transparency

Def-Logix recognizes that algorithm validation and effectiveness are crucial for ensuring the successful deployment of AI solutions like Crimson Raven. To ensure our algorithms perform accurately, fairly, and effectively, we use a comprehensive validation process that leverages the latest AI evaluation techniques. At the core of our validation strategy is DeepEval, an advanced evaluation framework for large language models (LLMs) that incorporates over 14 evaluation metrics, based on the latest research in AI evaluation. These metrics cover a broad range of considerations, from general accuracy to more advanced issues like bias and toxicity, allowing us to assess and refine our algorithms continuously.

1. **Algorithms in Crimson Raven:** Crimson Raven leverages advanced algorithms, including large language models (LLMs), machine learning (ML), natural language processing (NLP), and predictive analytics, to optimize service delivery, citizen engagement, and resource management. These algorithms work cohesively to process and analyze vast datasets in real-time, enabling automated decision-making and actionable insights that enhance operational efficiency. The key algorithms in Crimson Raven include:

- **Large Language Models (LLMs):** LLMs serve as the backbone for advanced NLP capabilities in Crimson Raven, enabling sophisticated natural language understanding and generation. These models allow the system to interpret complex citizen inquiries, provide accurate and context-aware responses, and improve conversational interfaces for citizen engagement.
- **Predictive Analytics:** Crimson Raven uses predictive analytics to forecast trends and outcomes by analyzing historical data. These algorithms help organizations proactively address issues such as demand surges, service bottlenecks, and efficient resource allocation, enabling informed, data-driven decisions.
- **NLP Algorithms:** Integrated with LLMs, NLP algorithms process unstructured text data to improve citizen interactions. They enable Crimson Raven to understand natural language inputs, deliver precise responses, and support multilingual and context-sensitive communication, improving accessibility and user satisfaction.
- **Machine Learning Models:** Both supervised and unsupervised learning methods are employed to detect patterns, identify anomalies, and continuously refine the system's performance. Reinforcement learning techniques may also be applied to adapt decision-making processes over time based on user interactions and evolving needs.

2. **Bias Mitigation and Ethical Outcomes:** Def-Logix's commitment to fairness and ethical AI is reflected in our deliberate approach to mitigate bias and ensure that the system operates equitably across all user demographics. To ensure that Crimson Raven's algorithms perform accurately, fairly, and effectively, we employ a rigorous validation process using the latest AI evaluation techniques. This process includes the use of *DeepEval, a comprehensive evaluation framework for large language models (LLMs), that incorporates over 14+ LLM evaluation metrics*, updated with the latest research in the field. Some of the metrics we use include:

- **G-Eval, Summarization, Hallucination, Faithfulness:** These metrics assess the accuracy, reliability, and contextual relevance of the model's outputs.
- **Answer Relevancy, Contextual Recall, and Contextual Precision:** These metrics ensure that the system's responses are pertinent and accurate within the context of the user's query.
- **RAGAS (Retrieval-Augmented Generation), Bias, Toxicity:** These advanced metrics allow us to assess the potential for bias and toxicity in the system's output, ensuring ethical and non-discriminatory interactions.



3. **Algorithm Validation and Effectiveness:** Ensuring that our algorithms perform effectively, fairly, and without unintended biases requires rigorous validation and testing processes. At Def-Logix, we use a combination of the following methods to validate and refine Crimson Raven’s algorithms:

Table 6 - Def-Logix Algorithm Validation Methods and Effectiveness

Validation Method	Description	Purpose
A/B Testing	Controlled experiments comparing different algorithm versions to observe performance differences. It helps refine decision-making capabilities.	Validates model improvements and ensures updates lead to measurable, positive enhancements.
Cross-Validation (k-Fold)	Partitioning the dataset into multiple subsets and testing the model on each to prevent overfitting and ensure robustness.	Ensures algorithms generalize well to new data and prevents model overfitting.
Fairness Audits	Regular audits using fairness metrics like Demographic Parity and Equal Opportunity to evaluate and address any biases in algorithmic decisions.	Ensures that the algorithms treat all groups equitably and identify any unintended biases.
Performance Monitoring	Real-time monitoring tools track algorithm performance, including operational efficiency and accuracy, detecting any performance deviations.	Ensures the system operates optimally and identifies any operational issues or inefficiencies.

Def-Logix ensures that Crimson Raven remains a high-performing, fair, and ethical AI solution by leveraging advanced evaluation metrics like those provided by DeepEval. Using bias mitigation techniques, ongoing model refinement, and rigorous validation processes, Def-Logix guarantees that the platform consistently upholds the highest standards of accuracy, fairness, and transparency. This approach enables Crimson Raven to deliver reliable, impactful, and trustworthy outcomes for both organizations and citizens.

4.3.9 Continuous Improvement

Crimson Raven is built with a focus on continuous improvement, ensuring that the solution evolves to meet the changing needs of users and adapts to emerging trends. The platform includes mechanisms that facilitate ongoing learning and performance enhancement, allowing algorithms to refine their capabilities based on real-time data, user interactions, and feedback. Key elements of our continuous improvement framework include:

1. **Adaptive Machine Learning Models:** The core of Crimson Raven’s continuous improvement lies in its adaptive machine learning models. These models are designed to learn from every user interaction and transaction, allowing them to become smarter and more efficient over time. As new data is collected, the algorithms analyze this information to identify patterns, improving decision-making, response accuracy, and service delivery efficiency.
2. **User Feedback Integration:** Crimson Raven actively integrates user feedback to improve its performance. Users can rate AI interactions and provide suggestions, which are automatically processed by the system. This feedback loop allows the platform to recognize areas of improvement and adjust the algorithms accordingly. As users engage with the system, the platform's responses and capabilities are refined to better meet their needs.
3. **Real-Time Performance Monitoring:** The solution includes real-time performance monitoring tools that track system effectiveness and efficiency. By analyzing key performance indicators (KPIs) and service outcomes, Crimson Raven automatically identifies opportunities for optimization. When

performance deviates from desired standards, the system adjusts its processes to realign with objectives, ensuring consistent service quality.

4. **A/B Testing and Experimentation:** Crimson Raven incorporates A/B testing and experimentation frameworks, allowing the system to test different approaches to service delivery, data processing, and user interaction. This testing is continuously conducted in a live environment, enabling the solution to determine the most effective methodologies and incorporate successful strategies into its operational framework.
5. **Model Retraining and Updates:** The platform continually retrains its machine learning models using the latest data and insights. This ensures that Crimson Raven stays up-to-date with evolving trends, user expectations, and operational demands. Model retraining is conducted in a systematic and controlled manner to ensure that improvements are effectively incorporated without disrupting service quality.
6. **Knowledge Base Expansion:** Crimson Raven's knowledge base is constantly updated as the system learns from user interactions and feedback. This evolving knowledge base supports the AI's ability to handle more complex queries and offer more tailored responses over time. Additionally, the platform continuously expands its repository of best practices, enabling it to provide better guidance and optimized solutions for users.

By embedding continuous learning and improvement mechanisms, Def-Logix will ensure that the solution not only meets the immediate needs of its users but also evolves in response to changing demands and advancements in AI technology. This dynamic approach guarantees that the system remains a high-performance tool capable of delivering sustained value over time.

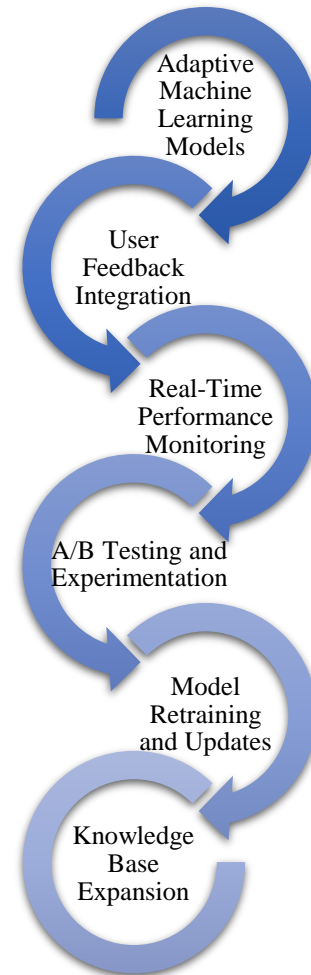


Figure 5 - Crimson Raven Continuous Improvement Framework.

4.3.10 Interoperability

Crimson Raven is designed with robust interoperability capabilities to seamlessly integrate with a wide array of existing digital infrastructures. Our solution will ensure smooth interaction with various government systems, allowing organizations to maximize their current investments while future-proofing their systems for evolving needs. Below is an outline of how Crimson Raven will achieve high interoperability, ensuring effective integration with your current systems and supporting scalable future integration.

1. **Adherence to Open Standards:** Crimson Raven is built on open standards to ensure compatibility with a wide range of systems and platforms. The use of industry-standard protocols such as RESTful APIs, JSON, and XML ensures that the solution can interface seamlessly with existing software

architectures, including legacy systems. Our commitment to open standards guarantees that Crimson Raven can integrate into diverse environments, reducing friction and enabling smooth data exchange.

2. **API Capabilities:** A key element of Crimson Raven’s interoperability is its comprehensive API framework. The platform offers robust and well-documented APIs that facilitate easy and secure data exchange between Crimson Raven and external systems. These APIs cover a broad range of functions, including:

- **Data Ingestion:** Allowing the import of data from external sources like case management, HR management, and utility billing systems.
- **Data Export:** Enabling the export of processed data to various downstream systems.
- **Real-Time Communication:** Facilitating real-time communication between Crimson Raven and external applications (e.g., chatbots, and service platforms).
- **User Management:** Allowing the synchronization of user identities with Identity and Access Management (IAM) systems.

3. **Data Format Compatibility:** Crimson Raven will support multiple data formats, ensuring that data can be exchanged without issues across different systems. Some of the formats supported will include:

- **Structured Data:** JSON, XML, CSV
- **Unstructured Data:** Text, log files, emails
- **Multimedia Data:** Images, audio, and video for service requests, citizen feedback, etc.

This flexibility in data formats allows Crimson Raven to integrate effectively with diverse systems, including those that might use proprietary data formats or legacy systems.

4. **Scalability to Support Future Integration:** As organizations grow and evolve, so will their infrastructure and integration needs. Crimson Raven will be designed to accommodate new systems, emerging technologies, and additional service requirements. The platform’s modular architecture will allow new integrations to be added as necessary, without disrupting ongoing operations. Whether integrating with a new case management system, upgrading security protocols, or adopting newer technologies like IoT or blockchain, Crimson Raven will scale to meet these needs with minimal effort.

5. **Interoperability Testing Protocols:** Before deployment, Crimson Raven will undergo rigorous interoperability testing to ensure flawless integration with existing systems. Our testing protocol will include the following phases:

- **Compatibility Testing:** Verifying that Crimson Raven communicates correctly with external systems using the supported data formats and APIs.
- **Load Testing:** Ensuring that Crimson Raven can handle a high volume of requests and interactions without degradation of performance.
- **Security Testing:** Testing all APIs and data exchanges for potential vulnerabilities, ensuring that data remains secure during transmission and processing.
- **End-to-end Testing:** Validating the entire integration process from data collection to processing and reporting to ensure the system functions as expected in real-world conditions.

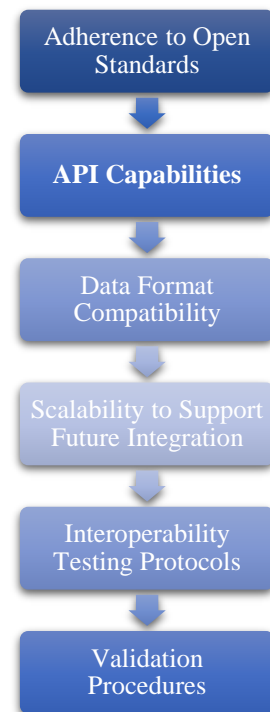


Figure 6 - Crimson Raven Interoperability Framework



- 6. Validation Procedures:** Once the interoperability testing is complete, the validation procedures will ensure the integrity of the integration. We employ a rigorous validation process using the latest AI evaluation techniques. This process includes the use of DeepEval, a comprehensive evaluation framework for large language models (LLMs), that incorporates over 14+ LLM evaluation metrics, updated with the latest research in the field.
- **Automated Data Validation:** Ensures the accuracy and completeness of data as it flows between Crimson Raven and external systems.
 - **Manual Review:** Post-integration, manual reviews of specific high-risk areas are conducted to ensure correct system behavior.
 - **Continuous Monitoring:** Ongoing monitoring tools check the status of all integrations, immediately alerting teams to any discrepancies or failures.

Crimson Raven will be designed to provide exceptional interoperability with existing systems, ensuring seamless integration, scalability, and flexibility for future requirements. By adhering to open standards, offering robust API capabilities, and undergoing rigorous testing, Crimson Raven will guarantee efficient, secure, and reliable integrations that support long-term success and operational continuity.

4.3.11 Quality Control

Ensuring the consistent performance and reliability of the solution is critical to maintaining high standards and meeting performance expectations. Def-Logix has implemented a comprehensive quality control (QC) framework for the Crimson Raven platform that includes both proactive and reactive measures. Our quality control process spans the entire lifecycle of the project, from initial design and development to ongoing maintenance and updates.

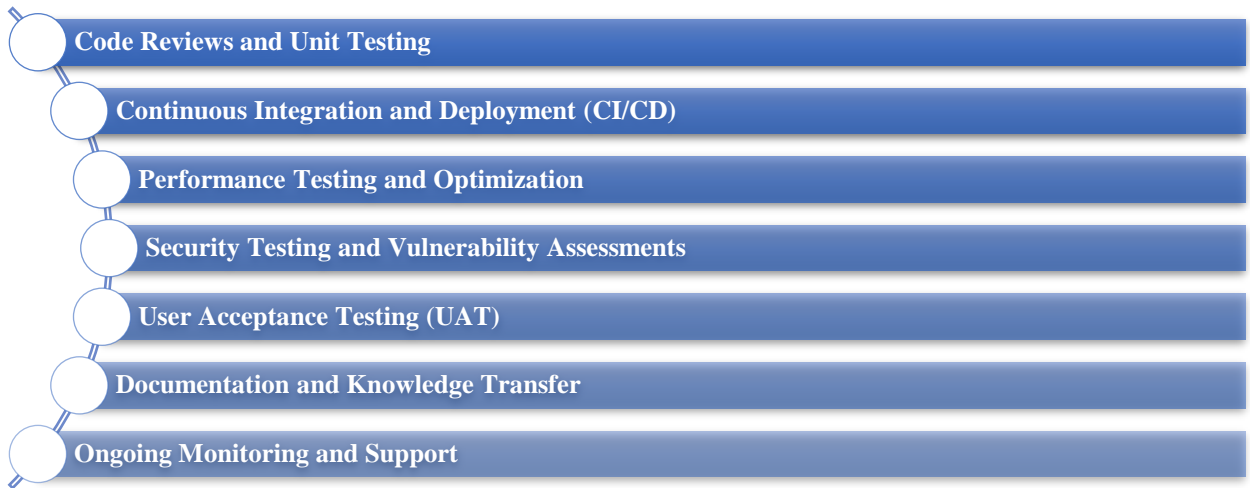


Figure 7 - Quality Control

- 1. Code Reviews and Unit Testing:** Def-Logix will establish a robust Code Review and Unit Testing process for all Crimson Raven development activities. Every code change will undergo thorough peer reviews to ensure compliance with best coding practices, security standards, and performance requirements. These reviews aim to identify issues early, including logic errors, security vulnerabilities, and optimization opportunities. In parallel, automated unit testing will be conducted on all components to verify their functionality and consistency. These tests will be executed regularly throughout the development cycle, ensuring high-quality, error-free, and optimized code from the ground up.



2. **Continuous Integration and Deployment (CI/CD):** Our **CI/CD pipeline** will ensure continuous testing, integration, and delivery of Crimson Raven components. Automated build and deployment processes will be used to integrate new features seamlessly while maintaining the integrity of the entire solution. Each code commit will trigger a **build** that runs automated unit tests, integration tests, and security checks, ensuring any issues are detected early. With CI/CD, Def-Logix can deliver updates quickly, ensuring reliability and minimizing deployment risks, while preventing system conflicts and ensuring seamless integration of all components.
3. **Performance Testing and Optimization:** Performance testing will be conducted regularly to ensure that Crimson Raven can handle high volumes of data, traffic, and user interactions. This will include stress tests to determine the system's capacity limits and load tests to simulate different usage scenarios. Key performance indicators, such as response time, throughput, and resource utilization, will be measured to identify bottlenecks. Based on the results, we will implement **optimization strategies**, such as database indexing, code refactoring, and caching techniques, to improve system performance and ensure scalability.
4. **Security Testing and Vulnerability Assessments:** Def-Logix will conduct comprehensive security testing to identify and address vulnerabilities within the Crimson Raven platform. This will involve regular vulnerability assessments using both automated and manual methods to ensure the solution meets security best practices. We will also perform penetration testing to uncover potential weaknesses that could be exploited by malicious actors, following industry standards like the OWASP Top 10 to safeguard both data and infrastructure from cyber threats.
5. **User Acceptance Testing (UAT):** To ensure that Crimson Raven meets the functional and operational needs of users, Def-Logix will engage with stakeholders in User Acceptance Testing (UAT). This phase will involve real-world users validating the platform's features, usability, and performance. Feedback from UAT will be used to make necessary adjustments, ensuring the solution meets the end-users expectations and requirements. UAT will also include scenario-based testing, where users test the platform with actual data and workflows to confirm that it operates seamlessly in real-world conditions.
6. **Documentation and Knowledge Transfer:** Def-Logix will provide comprehensive **documentation** throughout the development lifecycle. This includes detailed **technical documentation** for the code, architecture, and system configurations, ensuring that all components of Crimson Raven are well-understood and can be maintained effectively. We will also provide user guides and training materials for end-users to ensure they can navigate the platform effectively. **Knowledge transfer** sessions will be held with client teams to ensure they are fully equipped to manage, maintain, and enhance the solution post-deployment.
7. **Ongoing Monitoring and Support:** After deployment, Def-Logix will implement **continuous monitoring** to ensure that Crimson Raven remains functional and high-performing. This will include monitoring for system errors, performance issues, and security threats. Crimson Raven's design allows for a robust feedback mechanism, ensuring that issues detected at any stage of the lifecycle—whether pre- or post-deployment—are swiftly addressed. This continuous improvement process is vital to delivering the high standards expected from government solutions. We will set up alerts for any issues that require attention and provide **proactive support** to resolve issues before they impact users. Regular **system audits** and **performance reviews** will be conducted to ensure that the platform evolves in line with changing needs and emerging challenges, providing a long-term, sustainable solution.

Def-Logix's commitment to quality control ensures that Crimson Raven continues to meet the highest performance standards throughout its lifecycle. By integrating a multifaceted approach to QC and validation, we guarantee that the solution will consistently meet and exceed performance expectations, providing a reliable and robust service to our partners.



4.4 Data Governance and Cybersecurity Provisions

Our team has successfully implemented robust data governance frameworks for organizations such as the Department of Air Force (DAF) and the Department of Army (DOA), where we ensured the highest standards of data integrity, privacy, and security. Using our proven methodology, we will apply the same meticulous approach to your project, tailoring our practices to meet specific requirements while adhering to industry standards.

4.4.1 Data Governance

a) Data Integrity and Accuracy:

Def-Logix will implement a comprehensive data management framework that includes validation checks and error correction protocols to ensure the accuracy and integrity of data throughout its lifecycle. This will involve:

- 1) **Data Validation:** Automated validation processes will be established to check data against predefined criteria at the point of entry. This includes format checks, range checks, and consistency checks to ensure that only accurate data is captured.
- 2) **Error Correction Protocols:** In the event of data discrepancies, Def-Logix will employ error correction protocols that include automated alerts for anomalies, manual review processes, and corrective actions to rectify any identified issues.
- 3) **Regular Data Audits:** Scheduled audits will be conducted to assess data integrity, identify potential inaccuracies, and implement corrective measures as necessary.

b) Data Privacy and Compliance:

Def-Logix is committed to adhering to all relevant data privacy laws and regulations, including GDPR and CCPA. Our approach includes:

- 1) **Data Anonymization and Pseudonymization:** We will implement techniques for anonymizing and pseudonymizing personal data where applicable, ensuring that sensitive information is protected while still allowing for data analysis.
- 2) **User Consent Management:** A robust consent management system will be established to ensure that user consent is obtained before data collection and processing. This system will document consent records and provide users with clear options to withdraw consent at any time.
- 3) **Compliance Training:** Regular training sessions will be conducted for all employees to ensure they are aware of data privacy regulations and the importance of compliance.

c) Data Access Controls:

To protect sensitive data, Def-Logix will define and implement strict role-based access controls (RBAC) along with multi-factor authentication (MFA):

- 1) **Role-Based Access Control (RBAC):** Access to data will be restricted based on user roles within the organization. Each role will have specific permissions tailored to the needs of the job function, ensuring that only authorized personnel can access sensitive information.
- 2) **Multi-Factor Authentication (MFA):** MFA will be required for accessing sensitive data systems. This will involve a combination of something the user knows (password), something the user has (security token or mobile device), and something the user is (biometric verification) to enhance security.

d) Data Retention and Disposal:



We will establish clear data retention policies that outline how long data will be stored and the methods for secure disposal:

- 1) **Data Retention Policy:** We will define retention periods based on regulatory requirements, business needs, and best practices. Data will only be retained as long as necessary for its intended purpose.
- 2) **Secure Disposal Methods:** Once data is no longer needed, it will be disposed of securely using methods such as data wiping, physical destruction of storage media, or secure deletion protocols to prevent unauthorized access or recovery.

e) Data Auditing and Monitoring

Def-Logix will implement a robust auditing and monitoring framework to track data usage and access:

- 1) **Regular Audits:** We will conduct regular audits of data access logs and usage patterns to ensure compliance with access controls and identify any unauthorized access attempts.
- 2) **Logging Mechanisms:** Comprehensive logging mechanisms will be established to track all data access and modifications. These logs will be monitored in real-time for suspicious activity, with alerts generated for any anomalies detected.
- 3) **Continuous Improvement:** The auditing process will include feedback loops for continuous improvement, allowing us to refine our data management practices based on audit findings.

4.4.2 Cybersecurity

Def-Logix has successfully delivered cybersecurity services to various federal organizations, including AFLCMC, DHS, and DISA, ensuring robust protection against evolving threats. Our proven track record in implementing comprehensive security frameworks highlights our expertise in safeguarding critical data and systems. We have consistently met industry standards and regulatory requirements, strengthening our clients' cybersecurity posture. This experience equips us with the skills necessary to address complex security challenges, ensuring effective threat detection, response, and ongoing protection.

a) Threat Detection and Response:

Def-Logix will implement advanced AI-driven threat detection systems designed to identify and respond to potential security breaches in real-time. Our approach includes:

- 1) **AI-Driven Monitoring:** We will deploy machine learning algorithms that analyze network traffic and user behavior to detect anomalies indicative of security threats. These systems will continuously learn from new data, improving their accuracy over time.
- 2) **Identity Verification Mechanisms:** Robust identity verification protocols will be integrated into our access control systems. This includes multi-factor authentication (MFA) and biometric verification to ensure that only authorized personnel can access sensitive information.
- 3) **Incident Response Protocols:** We will define comprehensive incident response protocols that specifically address identity-related breach scenarios. These protocols will include steps for containment, eradication, recovery, and communication. Regular testing of these protocols through tabletop exercises and simulations will ensure preparedness for evolving security threats.

b) Encryption

To protect sensitive data, Def-Logix will ensure end-to-end encryption for data both in transit and at rest:

- 1) **Industry-Standard Encryption Algorithms:** We will utilize strong encryption standards such as AES-256 for data at rest and TLS (Transport Layer Security) for data in transit. RSA-2048 will be



employed for secure key exchange, while SHA-256 and SHA-512 will be used for hashing sensitive information.

- 2) **Key Management Practices:** A robust key management system will be established to handle encryption keys securely. This includes regular key rotation, secure storage, and strict access controls to prevent unauthorized access to encryption keys.

c) **Vulnerability Management**

Def-Logix is committed to maintaining a proactive approach to vulnerability management:

- 1) **Regular Vulnerability Assessments:** We will conduct comprehensive vulnerability assessments on a quarterly basis, utilizing automated tools to identify potential weaknesses in our systems.
- 2) **Penetration Testing:** Annual penetration testing will be performed by third-party security experts to simulate real-world attacks and identify vulnerabilities that may not be detected through automated assessments.
- 3) **Timely Patching and Updates:** A structured patch management process will be implemented to ensure that all software and systems are updated promptly in response to identified vulnerabilities. This includes prioritizing critical patches based on risk assessments.

d) **Security Governance Framework**

We will establish a robust security governance framework that outlines our security policies, procedures, and responsibilities:

- 1) **Policy Development:** We will develop comprehensive security policies that cover all aspects of cybersecurity, including data protection, access control, incident response, and compliance with relevant regulations.
- 2) **Continuous Compliance Monitoring:** Regular audits and assessments will be conducted to ensure adherence to security standards and best practices. This includes compliance with frameworks such as NIST Cybersecurity Framework and ISO 27001.
- 3) **Roles and Responsibilities:** Clear roles and responsibilities will be defined within the organization to ensure accountability for cybersecurity practices at all levels.

e) **Risk Management**

Def-Logix recognizes the importance of effective risk management in safeguarding our AI solutions:

- 1) **Risk Identification and Assessment:** We will conduct thorough risk assessments to identify potential risks associated with our AI solutions. This includes evaluating threats related to data privacy, system integrity, and operational continuity.
- 2) **Risk Mitigation Strategies:** Based on the identified risks, we will develop and implement risk mitigation strategies tailored to address specific vulnerabilities. This includes establishing a disaster recovery plan (DRP) that outlines procedures for restoring operations in the event of a significant incident.
- 3) **Root-Cause Analysis (RCA):** Following any security incident, a root-cause analysis will be conducted to identify underlying issues and prevent recurrence. Lessons learned from these analyses will inform future risk management strategies.

a) **Training and Awareness**

To foster a culture of cybersecurity awareness, Def-Logix will provide regular training programs for all staff:



- 1) **Cybersecurity Training Programs:** Comprehensive training sessions will be conducted bi-annually to educate staff on security best practices, including recognizing phishing attempts, secure password management, and safe data handling procedures.
- 2) **Awareness Campaigns:** Ongoing awareness campaigns will be implemented to keep cybersecurity top-of-mind for employees. This includes newsletters, posters, and interactive workshops that highlight current threats and preventive measures.
- 3) **Assessment of Knowledge:** Regular assessments will be conducted to evaluate staff understanding of cybersecurity protocols, ensuring that knowledge is retained and applied effectively.

Def-Logix is committed to building a comprehensive data security and cybersecurity framework that ensures the integrity, privacy, and accessibility of data while effectively identifying and addressing potential threats. By utilizing advanced threat detection systems, enforcing strict access controls, conducting regular audits, and providing continuous staff training, we protect our data and systems from emerging risks.

4.5 Performance Metrics

To effectively measure the success and performance of the Crimson Raven AI solution, we establish a robust framework for key performance indicators (KPIs) that align with the project goals. These KPIs are carefully designed to track the system's ability to improve public services, optimize data usage, and increase citizen engagement. Our approach to performance measurement includes accuracy, reliability, and continuous improvement, ensuring that the AI solution meets the required performance standards and evolves to meet changing needs over time. The following KPIs will be tracked to ensure Crimson Raven meets the required standards:

Table 7 - Crimson Raven Performance Metrics and KPIs

KPI	Description	Measurement Method
Accuracy of AI-driven Decisions	Measures how often the AI’s decisions align with the desired outcomes and expected results.	Performance benchmarking, A/B testing, and real-time monitoring.
Citizen Engagement	Tracks the level of interaction and engagement with citizens through AI-enabled interfaces.	Usage statistics, feedback surveys, and engagement rate analytics.
Service Optimization	Assesses how well the AI optimizes service delivery and resource allocation.	Efficiency metrics, service response time, resource utilization rate.
Bias Mitigation Effectiveness	Evaluates how effectively the AI prevents biased outcomes and ensures fairness.	Fairness audits, demographic parity tests, and regular audits.
Operational Efficiency	Measures the speed and reliability of AI-driven tasks, including process automation and real-time actions.	System uptime, response times, throughput rates, and failure rates.
Scalability	Measures the AI solution’s ability to handle increasing volumes of data and interactions over time.	Load testing, system scaling metrics, and resource usage metrics.
Feedback Loop Efficiency	Tracks the system's ability to incorporate user feedback into ongoing improvements and adjustments.	Frequency of updates, user satisfaction ratings, feedback processing speed.

To ensure our AI system delivers consistent accuracy and reliability, Def-Logix takes a proactive, multi-step approach. First, we set up real-time monitoring, keeping track of important metrics like decision accuracy, engagement, and service outcomes. If something isn't performing as expected, we get instant alerts, which allow us to act quickly and make corrections. We also use A/B testing regularly, comparing different versions of the algorithms to see which one works better, so we can ensure that any updates lead to measurable improvements. To further validate the system’s capabilities, we perform cross-validation and stress testing, simulating various scenarios to ensure the AI remains reliable, even during high-demand

periods. Finally, we build a feedback loop where performance data, user input, and system audits continuously inform improvements. This ensures the system keeps evolving, becoming smarter and more effective over time, while meeting the ever-changing needs of the users.

To ensure continuous improvement, Def-Logix will regularly update the AI model based on insights gathered from performance monitoring and real-world user interactions. These updates will be driven by continuous learning and feedback from system users and stakeholders, ensuring the solution adapts to evolving needs. To maintain fairness, we will conduct ongoing bias audits using fairness metrics and external experts, ensuring the system remains impartial. As data volumes and user interactions grow, we will monitor the scalability of the AI solution and make adjustments to ensure its reliability. Additionally, we will foster ongoing collaboration with stakeholders, keeping communication open to ensure the solution remains aligned with both technical and functional expectations, ultimately enhancing its performance over time. To effectively track and measure these KPIs, Def-Logix utilizes interactive dashboards that provide a clear and real-time view of performance across all metrics. Figure 8 illustrates a conceptual diagram depicting how our performance tracking and feedback loop operates.

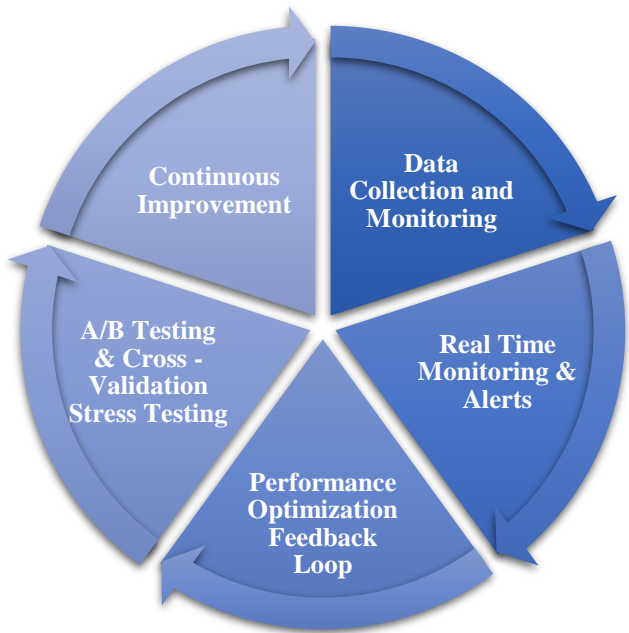


Figure 8 - Crimson Raven Performance Tracking and Feedback Loop

4.6 Risk Management

Crimson Raven adopts a proactive and comprehensive risk management framework to ensure the successful implementation and sustained performance of the project. This framework identifies potential risks, evaluates their impact, and applies tailored mitigation strategies to minimize disruptions while maximizing solution effectiveness. Below is a detailed breakdown of the risks and strategies, organized for clarity and accessibility.

Table 8 - Crimson Raven Risk Management Framework

Risk Area	Potential Risks	Mitigation Strategies
Data Security & Privacy	Unauthorized access, data breaches, non-compliance with regulations.	<ul style="list-style-type: none">• End-to-end encryption and multi-factor authentication.• Real-time monitoring with alerts.• Regular security audits and data anonymization.
Algorithm Bias & Ethics	Biased decision-making, lack of transparency, ethical concerns.	<ul style="list-style-type: none">• Fairness audits using industry metrics.• Diverse datasets to minimize bias.• Regular third-party reviews and transparent documentation of algorithms.
Performance & Scalability	Degraded performance under high workloads, and scalability issues.	<ul style="list-style-type: none">• Cloud-based infrastructure and load balancing.• Stress testing and real-time performance monitoring.



		<ul style="list-style-type: none"> Disaster recovery protocols for minimal downtime.
Integration Challenges	Difficulties integrating with legacy systems, compatibility issues, and high customization costs.	<ul style="list-style-type: none"> Pre-integration analysis and custom APIs. Incremental pilot testing. 24/7 technical support for integration issues.
User Adoption & Training	Resistance to new technology, insufficient training, and misalignment with user needs.	<ul style="list-style-type: none"> Stakeholder engagement early in the process Tailored training and user-friendly design Continuous feedback channels to refine adoption strategies.
Operational Downtime	Service disruptions, outages during updates, and limited contingency planning.	<ul style="list-style-type: none"> Scheduled updates during off-peak hours. Failover systems for continuity. Incident response plans and continuous testing to ensure high availability.
Regulatory Compliance	Non-compliance with laws, evolving regulatory standards, reputational risks.	<ul style="list-style-type: none"> Internal oversight committees and periodic reviews. Maintaining audit trails for transparency and accountability.

4.7 Compliance and Standards

Def-Logix confirms full adherence to all applicable regulations and standards, ensuring that our solution aligns with the highest levels of data privacy, security, and operational integrity. Crimson Raven is designed with compliance at its core, enabling seamless integration with frameworks and other regional and sector-specific standards. Our approach will encompass proactive monitoring, robust documentation, and stringent adherence to regulatory requirements, ensuring that every aspect of the solution is legally and ethically sound.

To maintain compliance, we will implement privacy-by-design principles, embedding data protection measures into every stage of the solution lifecycle. This will include advanced encryption protocols, access control mechanisms, and regular system audits. Our data processing workflows will be structured to ensure minimal data retention, and we will employ anonymization techniques where necessary to protect sensitive information. Furthermore, we will establish data subject access protocols that allow clients to respond promptly to user rights requests, such as data access or deletion.

Our commitment to regulatory compliance will be reinforced by periodic third-party audits and certifications. We will actively collaborate with compliance experts and legal advisors to ensure that our system remains aligned with evolving standards. Additionally, we will provide our clients with clear, transparent documentation and reporting capabilities, enabling them to demonstrate compliance during audits or inspections. By integrating these measures, we will ensure that Crimson Raven not only meets regulatory expectations but also fosters trust and accountability across all stakeholders.

5 Pricing

We have submitted this as a separate attachment – “**Exhibit 1 - Proposal Pricing**”.



6 Proposed Value-Add

Def-Logix offers innovative solutions and additional capabilities to enhance public sector operations beyond the scope of this RFP. Our value-added services include:

Technology Advisory	We offer expert Technology Advisory services to optimize system performance and seamlessly integrate new technologies. With a large, skilled team of SF Engineers, we tackle complex challenges, provide ongoing technical guidance, and test systems to ensure they meet your evolving needs.
Surge Capability	We offer flexible surge support to quickly scale resources for urgent project needs, ensuring efficient and timely outcomes during peak demands.
Cybersecurity	We implement robust cybersecurity solutions, conduct audits, and provide vulnerability assessments to safeguard your systems and data against emerging threats.
Comprehensive Training and Support	We deliver tailored training programs and ongoing support to maximize system adoption and operational efficiency, empowering your staff to fully leverage new technologies.

Figure 9 - Def-Logix Value-Added Services for Public Sector Operations

APPENDIX A.1

Pricing for TXShare Cooperative Purchase Program Participants

Service Category 1 – Artificial Intelligence (AI) Solutions for Public Sector Entities:

<div>Notes:</div> <div>1. This pricing sheet is an EXAMPLE of how pricing should be submitted for RFP 2025-018.</div> <div>2. Please provide unit pricing for each proposed item, including a percentage discount offering, if any.</div> <div>3. Use as many lines as necessary.</div> <div>4. Detail any additional information.</div>					
Description	Add additional description if necessary:	One-Time Cost	Unit Price	% Discount	Notes/Comments
1. Software Licensing and Subscription Costs: <i>Provide the cost breakdown for software licenses, subscriptions, or any other software-related fees.</i>	Crimson Raven Core AI Platform License. The unit price is the cost for 100 users per month	Free	\$ 500.00		Core software platform, scalable and modular
2. Implementation and Customization Costs: <i>Outline the costs related to the implementation of the AI solution, including setup, integration with existing systems, customization, and deployment.</i>	Custom configuration and deployment for Crimson Raven and selected modules	\$ 100,000.00			Covers foundational deployment, security integration, and agency-specific configuration
Automating Help Desk Support	AI Chatbots and Ticket Routing	\$ 150,000.00			Supports common issues resolution and smart routing to reduce ticket backlog
Streamlining IT Processes	Task Automation and Predictive Maintenance	\$ 100,000.00			Includes patch automation, backup scheduling, and log analysis
Creating Documentation	Knowledge Base Creation and Contextual Docs	\$ 100,000.00			Generates real-time documentation based on red team and ticketing data
Cybersecurity Threat Detection	Threat Monitoring, Anomaly Detection, Automated Response	\$ 150,000.00			Real-time alerting, threat scoring, auto-containment
Proactive Auditing & Cyber Defense	Continuous Security Audits, Predictive Defense, Compliance Automation	\$ 100,000.00			Supports NIST, HIPAA, GDPR; audit logs and predictive analytics
Total One Time Cost for Implementation and Modules		\$ 700,000.00			
Software Licensing and Subscription Costs with Modules	Monthly Subscription: This subscription will include Crimson Raven and all the modules stated above. The unit price is the cost for 100 users per month [\$12,000/year]		\$ 1,000.00		
3. Training and Support Costs: <i>Include costs for training government staff, technical support, and customer service, both during and after implementation.</i>	Per Year (10,000/month)		\$ 120,000.00		
4. Ongoing Maintenance and Updates: <i>Provide costs for ongoing software maintenance, updates, and any regular services required to keep the AI system running smoothly.</i>	Per Year (10,000/month)		\$ 120,000.00		
Total Cost of Software Licensing, Training and Support Costs and Ongoing Maintenance and Updates (Per Year)	\$12,000 + \$120,000 + \$120,000		\$ 252,000.00		
5. Optional Add-Ons or Features: <i>List any additional features or services available that are not included in the core proposal but can be added at an additional cost.</i>	Each additional features will take 3 months.	150000/module development			
6. Total Cost of Ownership (TCO): <i>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.</i>	Cost for 5 Years: 252,000 *5 (Per Year Cost: 252,000) + 700,000 + 20000		\$ 1,980,000.00		Optional: 150000/module development
7. Additional Costs (if applicable): <i>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.</i>		\$ 20,000.00	\$ 20,000.00		
After 6 months					
After the full-stack Crimson Raven solution is developed during the initial 6-month period , Def-Logix will offer an all-inclusive monthly subscription. This subscription covers access to all five key modules: Help Desk Automation, IT Process Optimization, Documentation Automation, Cybersecurity Threat Detection, and Proactive Auditing & Cyber Defense. The monthly fee includes licensing, maintenance, updates, and ongoing technical support. This pricing model ensures predictable costs and operational efficiency for NCTCOG. Optional features and module expansions can also be added as needed. The pricing structure is designed to be flexible; the total monthly subscription cost will be adjusted based on which modules and features NCTCOG chooses to include or exclude. This ensures that the agency only pays for the functionality it needs while retaining the option to scale or enhance the solution in the future.					
Plan	Description	Monthly Subscription Fee		Notes	
Crimson Raven – Full Stack	Full AI platform including Help Desk Automation, IT Process Optimization, Documentation Automation, Cybersecurity Threat Detection, and Proactive Auditing & Cyber Defense		1000/month		Covers all software access, infrastructure, support, upgrades, compliance reporting
Support & Maintenance	Helpdesk support, patching, monitoring, platform improvements, and model retraining		120000/year		No additional maintenance or support charges
Training & Updates	Continuous knowledge transfer, user enablement sessions, new feature rollouts		120000/year		Delivered quarterly or as-needed
Add-Ons (Optional)	Custom dashboards, mobile access, third-party tool integrations (Slack, Jira, etc.)		As Requested		Available per agency needs

APPENDIX A.2
Service Area Designation Forms



Exhibit 3: Service Area Designation Forms

EXHIBIT 3: SERVICE DESIGNATION AREAS

Texas Service Area Designation or Identification			
Proposing Firm Name:	Def-Logix, 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="" 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	Yes
2.	High Plains	Amarillo Lubbock	Yes
3.	Northwest	Abilene Wichita Falls	Yes
4.	Upper East	Longview Texarkana, TX-AR Metro Area Tyler	Yes
5.	Southeast	Beaumont-Port Arthur	Yes
6.	Gulf Coast	Houston-The Woodlands-Sugar Land	Yes
7.	Central Texas	College Station-Bryan Killeen-Temple Waco	Yes
8.	Capital Texas	Austin-Round Rock	Yes
9.	Alamo	San Antonio-New Braunfels Victoria	Yes
10.	South Texas	Brownsville-Harlingen Corpus Christi Laredo McAllen-Edinburg-Mission	Yes
11.	West Texas	Midland Odessa San Angelo	Yes
12.	Upper Rio Grande	El Paso	Yes

(Exhibit 3 continued on next page)



(Exhibit 3 continued)

Nationwide Service Area Designation or Identification Form			
Proposing Firm Name:	Def-Logix, 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="" 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	ALL	Yes
2.	Alaska	ALL	Yes
3.	Arizona	ALL	Yes
4.	Arkansas	ALL	Yes
5.	California	ALL	Yes
6.	Colorado	ALL	Yes
7.	Connecticut	ALL	Yes
8.	Delaware	ALL	Yes
9.	Florida	ALL	Yes
10.	Georgia	ALL	Yes
11.	Hawaii	ALL	Yes
12.	Idaho	ALL	Yes
13.	Illinois	ALL	Yes
14.	Indiana	ALL	Yes
15.	Iowa	ALL	Yes
16.	Kansas	ALL	Yes
17.	Kentucky	ALL	Yes
18.	Louisiana	ALL	Yes
19.	Maine	ALL	Yes
20.	Maryland	ALL	Yes

Page 39 of 40



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

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.

Caroline Frias-Costa
Signature of Authorized Person
Caroline Frias-Costa
Name of Authorized Person
Def-Logix, Inc.
Name of Company
01 May 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

Director of Contracts & Capture

Title

Def-Logix, Inc.

Agency

01 May 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

Carolina Frias-Costa

Name of Authorized Person

Def-Logix, Inc.

Name of Company

01 May 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

Carolina Frias-Costa

Name of Authorized Person

Def-Logix, Inc.

Name of Company

01 May 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).

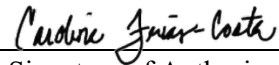
The entity identified below, through its authorized representative, hereby certifies that they do not boycott energy companies, and that they will not boycott energy companies during the term of the contract as prohibited by Chapter 809, Subtitle A, Title 8 of the Texas Local Government Code.

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

Carolina Frias-Costa

Name of Authorized Person

Def-Logix, Inc.

Name of Company

01 May 2025

Date

APPENDIX E
DEBARMENT CERTIFICATION

Paul A. Rivera _____ being duly
(Name of certifying official)
sworn or under penalty of perjury under the laws of the United States, certifies that neither


_____, 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
CEO & President

Title
01 May 2025

Date of Certification
Form 1734
Rev.10-91
TPFS

**APPENDIX E
DEBARMENT CERTIFICATION**

Paul A. Rivera being duly
(Name of certifying official)
sworn or under penalty of perjury under the laws of the United States, certifies that neither

_____, 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:

Paul A. Rivera

Signature of Certifying Official
CEO

Title
May 1, 2025

Date of Certification

Form 1734
Rev.10-91
TPFS