

TXShare

Your Public Sector Solutions Center

REQUEST FOR PROPOSALS

For

Artificial Intelligence (AI) Solutions for Public Sector Entities

RFP # 2025-018

Sealed proposals will be accepted until 2:00 PM CT, **January 17, 2025**, and then publicly opened and read aloud thereafter.

Def-Logix, Inc.

Legal Name of Proposing Firm

Sa Huynh

Contact Person for This Proposal

Proposal Manager

Title

210.800.7303

Contact Person Telephone Number

proposals@def-logix.com

Contact Person E-Mail Address

3463 Magic Drive, Ste.220

Street Address of Principal Place of Business

San Antonio

City/State

78229

Zip

3463 Magic Drive, Ste.220

Mailing Address of Principal Place of Business

San Antonio

City/State

78229

Zip

Carolina Frias-Costa

Point of Contact for Contract Negotiations

Director of Finance

Title

210.624.8064

Point of Contact Telephone Number

cfcosta@def-logix.com

Point of Contact Person E-Mail Address

Acknowledgment of Addenda (initial): #1 SLH #2 _____ #3 _____ #4 _____ #5 _____

NOTE: Any confidential/proprietary information must be clearly labeled as "confidential/proprietary". All proposals are subject to the Texas Public Information Act.

COVER SHEET

Authorized Representative



Table of Contents

1	Statement of Understanding.....	1
2	References.....	1
2.1	Reference #1 – Rob Dodson	1
2.2	Reference #2 – Nicholas Navarro	1
3	Project-Related Experience and Qualifications	2
3.1	Organization’s Capabilities and Experience	2
3.1.1	Technical Expertise.....	3
3.1.2	Project Management	4
3.1.3	Team Qualifications.....	5
3.1.4	Resume 1 – Paul Rivera.....	5
3.1.5	Resume 2 – Nicholas Navarro	6
3.1.6	Resume 3 – Noah Psutka	9
3.2	Relevant Past Projects.....	10
3.3	Background and Years in Business.....	10
3.4	Significant Requirements Not Met	11
4	Technical Proposal.....	11
4.1	Project Deliverables	11
4.1.1	Information Technology and Cybersecurity (IT).....	11
4.2	Technical Approach.....	12
4.2.1	Methodologies for design and development	13
4.2.2	Integration strategies with existing government systems	13
4.2.3	User-friendliness and accessibility considerations	14
4.3	Technical Requirements.....	15
4.3.1	Challenge-Specific Functionality.....	15
4.3.2	Scalability	15
4.3.3	Integration	15
4.3.4	Real-Time Analytics	15
4.3.5	Data Security and Privacy.....	15
4.3.6	Natural Language Processing Capabilities	16
4.3.7	Accuracy	16

4.3.8	Algorithm Transparency	17
4.3.9	Continuous Improvement.....	18
4.3.10	Interoperability.....	19
4.3.11	Quality Control	21
4.4	Data Governance and Cybersecurity Provisions.....	23
4.4.1	Data Governance.....	23
4.4.2	Cybersecurity	24
4.5	Performance Metrics	26
4.6	Risk Management	27
4.7	Compliance and Standards.....	28
5	Pricing	28
6	Proposed Value-Add	29
7	HUB	30
8	Required Attachments.....	31
	Attachment I: Instructions for Proposals Compliance and Submittal.....	31
	Attachment II: Certification of Offeror.....	32
	Attachment III: Certification Regarding Debarment	33
	Attachment IV: Restrictions on Lobbying.....	34
	Attachment V: Drug-Free Workplace Certification	35
	Attachment VI: Certification Regarding Disclosure of Conflict of Interest.....	36
	Attachment VII: Certification of Fair Business Practices.....	37
	Attachment VIII: Certification of Good Standing Texas Corporate Franchise Tax Certification	38
	Attachment IX: Historically Underutilized Businesses	39
	Attachment X: Federal and State of Texas Required Procurement Provisions	40
	Exhibit 1: Description of Desired Product Categories for Proposed Pricing.....	43
	Exhibit 3: Service Area Designation Forms	44

List of Figures

Figure 1 - Key Advantages of Def-Logix's Crimson Raven Solution.....	2
Figure 2 - Features of Crimson Raven (CR) and Crimson Crawler (CC)	3
Figure 3 - Project Management.....	5
Figure 4 - Crimson Raven's AI-Driven Citizen Engagement Framework.....	14
Figure 5 - Crimson Raven Continuous Improvement Framework.	19
Figure 6 - Crimson Raven Interoperability Framework	20
Figure 7 - Quality Control.....	21
Figure 8 - Crimson Raven Performance Tracking and Feedback Loop	27
Figure 9 - Def-Logix Value-Added Services for Public Sector Operations	29

List of Tables

Table 1 - Def-Logix: Areas of Specialization, Technologies, and Methodologies	4
Table 2 - AI-driven IT and Cybersecurity Enhancements for the Public Sector.	11
Table 3 - Def-Logix Design and Development Methodologies.....	13
Table 4 - Def-Logix Integration Strategy for Crimson Raven.....	14
Table 5 - Crimson Raven User-Friendliness and Accessibility Considerations	14
Table 6 - Def-Logix Algorithm Validation Methods and Effectiveness	18
Table 7 - Crimson Raven Performance Metrics and KPIs.....	26
Table 8 - Crimson Raven Risk Management Framework	27

1 Statement of Understanding

Def-Logix understands that the NCTCOG is seeking innovative AI-driven solutions to address key challenges faced by public sector entities. The goal is to enhance operational efficiency, improve service delivery, and foster innovation across municipalities, counties, school districts, and other government agencies. We recognize the importance of leveraging AI to optimize data usage, improve public services, and increase citizen engagement, and we are committed to providing solutions that meet these objectives effectively.

Def-Logix will provide targeted AI solutions addressing the operational challenges in **Information Technology and Cybersecurity (IT)**. Our solutions are designed to optimize workflows, enhance decision-making, secure digital assets, and drive operational resilience. By incorporating state-of-the-art AI technologies, we foster innovation and adapt to the evolving needs of public sector entities. We prioritize scalable, customizable solutions that can be tailored to meet the unique requirements of municipalities, counties, school districts, and other government entities. Def-Logix's approach ensures measurable improvements in service delivery, operational effectiveness, and cybersecurity resilience, aligning with the objectives of **Service Category #1, Artificial Intelligence (AI) Solutions** for Public Sector Entities.

2 References

2.1 Reference #1 – Rob Dodson

Organization Name	Def-Logix	
POC	Contact Person	Rob Dodson
	Phone Number	(210) 952-3820
	Email Address	rdodson@cyberopsacademy.com
Project Description		
Rob Dodson successfully organized and facilitated a dynamic Cyber Ops meetup, creating an interactive environment that enabled participants to engage directly with Crimson Raven, a cutting-edge AI-driven platform. Through hands-on exploration and practical application, attendees were not only able to test the platform's capabilities but also contribute insightful feedback based on their real-world experiences. This collaborative session exemplified Rob's skill in fostering engagement between users and advanced technologies. By seamlessly integrating technical expertise with user-centric facilitation, Rob ensured that the feedback collected during the meetup was both actionable and directly relevant to the ongoing development of Crimson Raven.		

2.2 Reference #2 – Nicholas Navarro

Organization Name	Def-Logix	
POC	Contact Person	Paul Rivera
	Phone Number	(210)-478-1369
	Email Address	privera@def-logix.com
Project Description		
As the main project manager for the development of Crimson Raven an innovative framework that offers a sophisticated framework that merges highly fine-tuned Large Language Models (LLMs) with Retrieval Augmented Generation (RAG) technology to provide expert domain knowledge in the cyber operations field., Nicholas oversees all aspects of the project and leverages his technical expertise to drive innovation. He is responsible for developing comprehensive project plans that outline objectives, timelines, and resource requirements, while also facilitating communication among cross-functional teams to promote collaboration and address challenges. Nicholas actively identifies potential risks to the project timeline and implements effective mitigation strategies. He regularly monitors project progress against established benchmarks, making necessary adjustments to ensure successful outcomes. Additionally, he maintains strong relationships with stakeholders, providing updates on project status and incorporating their feedback into the development process.		

3 Project-Related Experience and Qualifications

3.1 Organization's Capabilities and Experience

Def-Logix has developed **Crimson Raven (def-logix.ai)**, a cutting-edge AI solution designed to transform how cyber operators engage with critical data. Our team consists of highly skilled professionals with expertise in AI, machine learning, and cybersecurity, who have worked together to create this innovative platform. Crimson Raven combines advanced Large Language Models (LLMs) with Retrieval Augmented Generation (RAG) technology to provide real-time insights and support for red team operators. The system helps operators analyze and process vast amounts of data more efficiently, improving decision-making and operational performance. With our strong engineering team and ongoing commitment to innovation, Def-Logix continues to deliver powerful AI solutions tailored to meet the evolving needs of the cybersecurity field.

Crimson Raven is specifically tailored for red team operators, offering both instructional and conversational interaction modes, similar to ChatGPT. The platform enhances the functionality of operator UIs embedded within red team tools, allowing operators to efficiently search command references, obtain suggestions, and learn or execute specific Techniques, Tactics, and Procedures (TTPs). This dynamic framework is designed to assimilate critical data, including tactics from the MITRE ATT&CK framework, operator manuals, knowledgebases, and historical operation data, into an easily accessible and actionable format.

Proven Experience <ul style="list-style-type: none"> •Crimson Raven, our pre-built solution, integrates fine-tuned LLMs and RAG technology to enhance cyber operations efficiency.
Time-Saving Innovation <ul style="list-style-type: none"> •With Crimson Raven already developed, we enable rapid deployment, significantly reducing the time required for AI/ML system implementation.
Real-Time Monitoring <ul style="list-style-type: none"> •Our systems continuously track performance metrics, enabling the immediate detection of issues and guaranteeing the reliability and accuracy of operations in dynamic environments.
Seamless Integration <ul style="list-style-type: none"> •We specialize in effortlessly integrating AI/ML models into existing software systems, ensuring minimal disruption while maximizing the value of your current technological infrastructure.
Robust Data Management <ul style="list-style-type: none"> •We excel in preparing, cleaning, and organizing complex datasets, ensuring the accuracy and accessibility of critical data, which optimizes model performance and drives more reliable insights.

Figure 1 - Key Advantages of Def-Logix's Crimson Raven Solution

Our expertise is demonstrated through our ongoing maintenance and updates to def-logix.ai, which supports the pipeline for Computer Network Operations (CNO) Co-Pilot. This includes regular CI/CD pipeline updates every 2-4 weeks, ensuring peak system performance and adaptability in the face of evolving cybersecurity challenges.

Def-Logix has also developed **Crimson Crawler**, an advanced Open-Source Intelligence (OSINT) platform designed to deliver actionable insights into cybersecurity threats and vulnerabilities. Leveraging cutting-edge machine learning algorithms and state-of-the-art data aggregation techniques, Crimson Crawler systematically gathers and analyzes vast amounts of publicly accessible data from a variety of digital channels, including social media, online forums, dark web sources, and open databases.

The platform employs Large Language Model (LLM) based scraping technologies to extract and store website data in a centralized repository, which serves as a Retrieval-Augmented Generation (RAG) resource for AI-driven tasks. Crimson Crawler operates in two key modes:

1. **Repository Mode:** Collects and archives data in the RAG repository for use in AI-assisted analysis and intelligence generation.
2. **Ad Hoc Agent Mode:** Functions as an adaptive search engine, conducting real-time queries to address specific OSINT requirements.

With its customizable data visualization tools and automated reporting capabilities, Crimson Crawler enables security analysts to efficiently identify, prioritize, and mitigate emerging threats. By enhancing situational awareness and supporting data-driven decision-making, this platform represents a significant advancement in cybersecurity defense strategies.

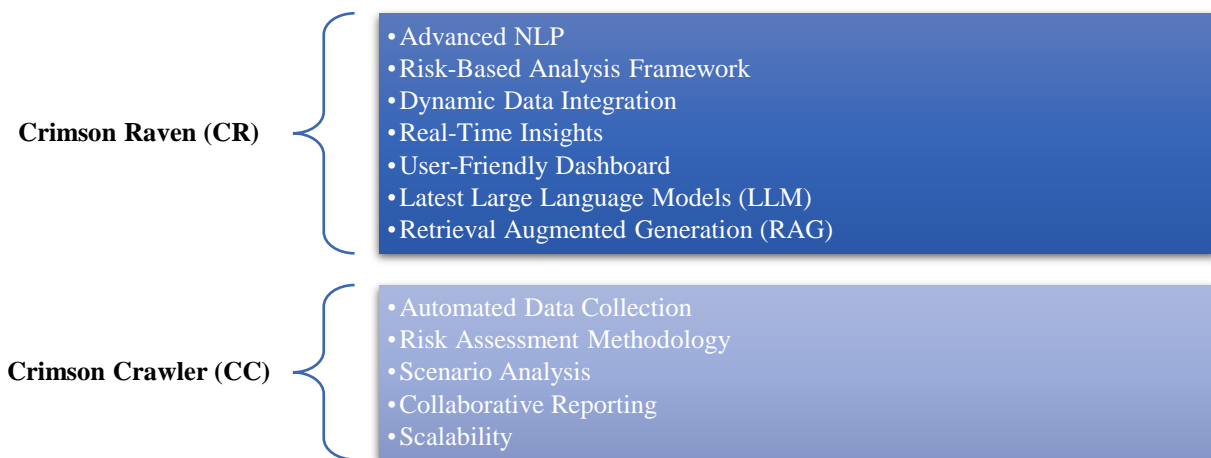


Figure 2 - Features of Crimson Raven (CR) and Crimson Crawler (CC)

Our solutions, **Crimson Raven (CR)** and **Crimson Crawler (CC)** are specifically designed to address the challenges of Computer Network Operations (CNO). Together, they deliver an AI-driven assistant for Red Team, Blue Team, and Open-Source Threat Intelligence operations.

- **Crimson Raven (CR)** leverages Natural Language Processing (NLP), LLMs, and RAG to analyze unstructured data from reputable vulnerability, cybersecurity, and cyber threat intelligence feeds. This automation streamlines CNO-related tasks, enabling faster threat detection and mitigation.
- **Crimson Crawler (CC)** automates the collection and analysis of open-source cyber threat intelligence, focusing on key factors such as recent incidents, cybercrime activities, and nation-state campaigns.

By combining these platforms, operators can efficiently assess, respond to, and report on cyber incidents, significantly enhancing operational agility and resilience in the face of evolving threats.

3.1.1 Technical Expertise

Def-Logix specializes in developing state-of-the-art solutions at the intersection of cybersecurity and artificial intelligence. Our team has built Crimson Raven (CR) and Crimson Crawler (CC), a cutting-edge AI platform that transforms the way cyber operators engage with critical data. Our team of highly skilled professionals, with deep expertise in AI, machine learning, and cybersecurity, has collaborated to create this innovative platform to improve the effectiveness and efficiency of cybersecurity operations. Below is an overview of the AI technologies and methodologies Def-Logix specializes in, which power Crimson Raven and other cybersecurity solutions.

Table 1 - Def-Logix: Areas of Specialization, Technologies, and Methodologies

Area of Specialization	Technologies	Methodologies
AI-Powered Threat Detection and Prevention	Machine Learning (ML)	Continuous data training and model improvement for evolving threats.
	Deep Learning	Real-time monitoring and alerting using AI-driven insights.
	Anomaly Detection	Identifying deviations from normal activity to flag potential threats.
Automated Incident Response	Natural Language Processing (NLP)	AI-driven automation for faster incident response.
	Robotic Process Automation (RPA)	Integration with SIEM systems for automated workflows.
Vulnerability Management and Prediction	Predictive Analytics	Proactive vulnerability scanning using AI-driven tools.
	AI for Penetration Testing	Continuous vulnerability assessments to prioritize risks.
AI-Enhanced Software Development	AI for Code Analysis	Automating code review processes for security vulnerabilities.
	DevSecOps Integration	Embedding AI into DevOps pipelines for secure coding practices.
AI-Driven Behavioral Analytics	User and Entity Behavior Analytics (UEBA)	Real-time monitoring of user and device behavior to detect threats.
	Contextual AI	Improving threat detection accuracy by understanding user context.
AI-Driven Network Security	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	Integration with next-gen firewalls for enhanced threat detection accuracy.
AI-Powered Threat Intelligence	AI for Threat Intelligence Feeds	Processing large volumes of threat data to provide actionable insights.
	Cyber Threat Hunting	Using AI to predict and identify advanced threats.
Crimson Raven-Specific Technologies	Large Language Models (LLMs)	Enhanced operator interaction with conversational AI interfaces.
	Retrieval Augmented Generation (RAG) technology	Using real-time insights and data retrieval from knowledgebases to improve decision-making.
Red Team Support	AI for Command Reference Search	Seamless integration with red team tools for efficient search and suggestion generation.
	Contextual AI for TTP Execution	Providing situational awareness by offering suggestions on specific Tactics, Techniques, and Procedures (TTPs).
Data Assimilation and Knowledge Management	Data Retrieval Systems	Assimilating critical data from various sources (e.g., MITRE ATT&CK framework, manuals, operator data).
	Knowledge Graphs	Structuring historical operation data, TTPs, and other cybersecurity intelligence for easier access.
Adaptive AI Framework	Adaptive Learning Algorithms	Continuously evolving decision-making capabilities to stay ahead of emerging cybersecurity threats and red team operations.

3.1.2 Project Management

Def-Logix has successfully managed various federal projects, including cybersecurity initiatives for AFLCMC and DoD. In addition, we developed and deployed Crimson Raven (CR) and Crimson Crawler

(CC), an in-house project that showcases our expertise in AI solutions. With a wealth of experience in managing both AI and cybersecurity, we consistently deliver high-quality results by expertly navigating complex requirements. Our approach ensures efficiency and innovation while fully complying with government standards. Below is an overview of the structured methodology we follow to guarantee the successful execution of each project, from planning to post-project evaluation:

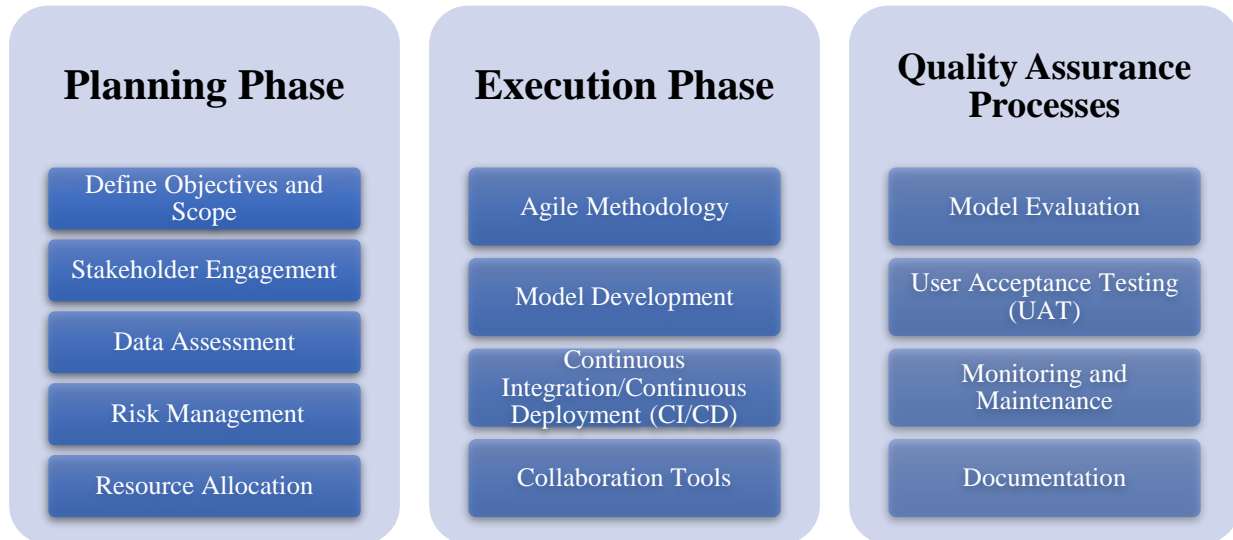


Figure 3 - Project Management

Def-Logix believes in continuous improvement and learning from every project. Following the successful completion of each AI project, such as **Crimson Raven**, we conduct a thorough post-project review to ensure ongoing growth and excellence in our delivery. This review begins with a **Performance Analysis**, where we rigorously compare the project outcomes with the initial objectives to evaluate success, identify lessons learned, and establish best practices for future projects. Additionally, we actively seek **Stakeholder Feedback** to gauge satisfaction levels and uncover areas for improvement. This invaluable input not only informs our approach to future AI projects but also drives enhancements in our processes, ensuring we continually meet and exceed stakeholder expectations. By integrating these insights into our future work, we strive to refine our strategies and maintain the highest standards in AI solution delivery.

3.1.3 Team Qualifications

Our team members are highly qualified professionals with extensive experience in advanced cybersecurity solutions, artificial intelligence, and Open-Source Intelligence (OSINT) systems. They have played an integral role in designing, developing, and implementing cutting-edge platforms such as Crimson Raven and Crimson Crawler, which enhance cyber operations efficiency and automate OSINT data collection and analysis. ***We have three key personnel for this project: Paul Rivera, Nicholas Navarro, and Noah Psutka.*** Each brings a wealth of expertise in areas such as AI-powered threat detection, vulnerability management, and advanced data aggregation methodologies, ensuring the successful execution of project objectives. Please see the attached resumes for detailed qualifications and experience of these individuals.

3.1.4 Resume 1 – Paul Rivera

Name & Proposed Role	Education
Paul Rivera Program Manager	<ul style="list-style-type: none"> Master of Science in Information Technology/Information Assurance Concentration - University of Texas at San Antonio, San Antonio, TX, 2009 Bachelor of Science in Computer Science - University of Texas at San Antonio, San Antonio, TX 1996

Summary	
<p>Founder of Def-Logix, Inc. with over 20 years of experience in cybersecurity. Adaptable and accomplished leader with expertise in operations, product development, and team building within startup and growth environments. Results-oriented trailblazer with a proven track record of securing government contracts and driving new product development in the competitive cybersecurity landscape. Sponsoring monthly CyberOps Academy meetups to enhance cybersecurity accessibility for novices. Expert in Information Technology with a specialization in computer and network security. Early career focused on developing Network and Host-based Intrusion Detection/Prevention Technologies (IDS/IPS), with extensive experience evaluating and testing a wide range of commercial security applications and appliances.</p>	
Employment History and Experience	
Company: Def-Logix, Inc.	2008 – Present
Designation: CEO & Owner	
<ul style="list-style-type: none"> Principal investigator on a DHS BAA-funded project to defend against zero-day exploits. Managed a team of software engineers developing HBSS modules for system information gathering. Managed the team of test engineers' setup of the HBSS test environment. Team lead and architect of a virtual environment for the detection and catalog of malicious email attachments. 	
Company: Endeavor Systems	2000 - 2010
Designation: Project Technical Lead / Consultant	
<ul style="list-style-type: none"> Principal investigator on a DHS BAA-funded project to defend against zero-day exploits. Managed a team of software engineers developing HBSS modules for system information gathering. Managed the team of test engineers' setup of the HBSS test environment. 	
Company: L-3 Communications	2005 – 2009
Designation: Principal Software/ Network Security Engineer	
<ul style="list-style-type: none"> Developed Cloudshield applications in RAVE and PacketC focusing on VOIP. Subject matter expert in assessing web servers and web applications. Tools used were Nessus, Wikto, nmap, Metasploit, fping, and hping. 	
Company: Titan Systems	2003 - 2005
Designation: Senior Software Developer	
<ul style="list-style-type: none"> Conducted System Vulnerability Assessments for USAF computer networks. Tested and evaluated commercial off-the-shelf intrusion prevention systems. Developed correlation engine/service for customers which mapped customer product events to the SANS Top 20 computer vulnerabilities. 	
Company: Self-Employed	2002 - 2003
Designation: IT Security Consultant	
<ul style="list-style-type: none"> Assessed network security and developed risk mitigation plans and security policies for HIPAA compliance for various clients (pharmacies and small medical practices). Researched & analyzed vulnerabilities & exploits for network intrusion detection system signature development. 	
Company: Symantec	2002 - 2002
Designation: Senior Software Developer / Independent Consultant	
<ul style="list-style-type: none"> Developed an Automated Test Framework for the Intrusion Detection Signature Team. The Test Framework validated signature accuracy and tested the signature language capabilities of the intrusion detection engineer. 	
Company: Viridian Information Solutions	1999 - 2002
Designation: Software Engineer	
<ul style="list-style-type: none"> Team lead on the integration of third-party network intrusion detection systems into CIDDS utilizing SYSLOG and SNMP features for Veteran Administration Hospital Networks. Researched and tested network protocols and network applications to determine flaws and vulnerabilities. 	

3.1.5 Resume 2 – Nicholas Navarro

Name & Proposed Role	Education
----------------------	-----------

Nicholas Navarro AI SME	<ul style="list-style-type: none"> ➤ Graduated with a 4.0 GPA. Norwich is an NSA-approved Center of Academic Excellence for InfoSec. - Norwich University Master of Information Assurance (MSIA), Sept. 2005 – June 2007. ➤ Bachelor of Science in Computer Science, 2002 - Park University, Graduated with a 4.0 GPA.
Summary	
<p>Dynamic and results-driven Senior Cyber Security Director with over 20 years of extensive experience in the cybersecurity domain. Currently serving as the Director of Technology at Def-Logix, specializing in cyber defense solutions for government clients, with a strategic focus on commercializing innovative technologies. Expert in research and development, leading initiatives in network forensics, malware analysis, red team tool development, and low-level defense solutions, including software-based kernel drivers and EFI firmware development. Previous experience as a Network Security Engineer involved deploying and testing a wide range of security technologies. Hands-on red team experience, including participation in the 2015 Southwest Regional and National Collegiate Cyber Defense Competitions (CCDC). Played a pivotal role in commercial incident response efforts, notably as the first employee onsite during the TJX Companies credit card breach in 2006, where expertise in network and digital forensics was critical. Recently developed a strong interest in machine learning and data science, applying these skills to enhance malware and network traffic analysis for various research projects.</p>	
Core Competencies	
<ul style="list-style-type: none"> • Cybersecurity Leadership • Research and Development • Red Team Operations • Incident Response • Software Development 	<ul style="list-style-type: none"> • Security Technology Deployment • Machine Learning and Data Science • Collaboration and Communication • Strategic Planning • Continuous Learning
Certifications	
<ul style="list-style-type: none"> • SANS GIAC Reverse Engineering Malware Certification Course (GREM) (2011 - Current) • ISC2 CISSP Security Certification (2002 - Current) • Various Pluralsight and SANS Webcasts related to development and cybersecurity • Black Hat USA Exploit Laboratory Black Belt Edition Training Class (2013) • Harris APPSEC Malware analysis crash course • Offensive Security WIFU wireless hacking certification • Black Hat USA Exploit Laboratory Training Class (2008) • Certified Ethical Hacker V5 (2008) • Internal Reverse Engineering Class with IDAPro (2007) • ArcSight Analyst Certification (2002) • ArcSight Administrators Certification (2002) • McAfee Intrushield Engineers Course (2006) 	
Employment History and Experience	
Company: Def-Logix	2019 – Present
Designation: Director of Research and Development	
<ul style="list-style-type: none"> • Team Leads on the project which focuses on leveraging cutting-edge .NET technology to build a red team agent that can be deployed on Windows systems covertly and achieve red team mission objectives. • Senior tech advisor and subject matter expert of red team tool development and integration into red team command-and-control platforms for government cyber exercises. • Senior tech advisor on web-based applications that use cloud technologies to stage C2 frameworks on Amazon Web Services EC2 instances in an automated fashion. • Overarching senior tech advisor on most Def-Logix anti-malware, red team projects, and research and development-related projects. 	
Company: Def-Logix	2018 - 2019
Designation: Director of Technology	

<ul style="list-style-type: none"> • Architected Anti-Malware Solutions: Led the development of the Entrap anti-malware endpoint solution for Windows and Linux, utilizing behavior detection and kernel modules to identify malicious activity, including automation of deployment and testing with Vagrant and Ansible. • Red Team Tool Development: Managed projects to create custom red team tools for testing in-house anti-malware technologies and automated testing environments using Government-off-the-shelf (GOTS) products. • Integrated Cybersecurity Frameworks: Prototyped an ELK stack solution with McAfee DXL for sharing malware-related events and indicators of compromise (IOCs) across cybersecurity applications, enhancing data analysis capabilities. • TLS Inspection Tool Development: Oversaw the creation of a tool for intercepting and inspecting encrypted TLS session data at Windows endpoints, supporting IDS signature rules to identify malicious traffic. • Firmware Integrity Monitoring: Directed a project to develop tamper-resistant components compliant with UEFI standards, enabling pre-boot integrity checks and real-time monitoring of critical Windows services against malware tampering. 	
Company: Def-Logix, Inc.	2016 – 2018
Designation: Chief Architect	
<ul style="list-style-type: none"> • Entrap Anti-Malware Development: Contributed to the architecture and development of the Windows Entrap anti-malware solution, utilizing API inspection and process monitoring, enhanced under a DHS-funded initiative to detect advanced malware through real-time behavioral analysis. • Cybersecurity Data Integration: Designed a web-based server application for integrating Entrap event data into CyBOX and STIX formats, facilitating the exchange of cybersecurity information on malware and attacks. • DOD Integration Modules: Developed integration modules for the Department of Defense's Host-Based Security System (HBSS) using McAfee ePolicy Orchestrator, achieving certification for commercial sale as a McAfee Security Innovation Alliance product. • GOTS Cyber Hunt Tool Testing: Directed testing teams to successfully submit an integrated version of Entrap for certification at the Air Force Integration Test and Evaluation Center (ITEC). • DARPA Plan X Development: Led the design and development of HBSS integration modules and Python/LUA applications for the DARPA Plan X cyber-warfare platform, enhancing asset management and operational capabilities within the DOD. 	
Company: Root9b, Inc.	2016 – 2016
Designation: Director, Enterprise Solutions Consulting Practice	
<ul style="list-style-type: none"> • Developed a Java FX 8 graphical application and back-end code that automatically generated a virtual range for cyber operators for training courses using a VMware vSphere environment. 	
Company: Def-Logix, Inc.	2010 – 2016
Designation: Information Security Developer	
<ul style="list-style-type: none"> • Crypto Interception Tool Development: Designed a Python tool for intercepting encrypted command-and-control channels used by malware. • Automated Deployment Tools: Created a network-based automation suite for Linux and Solaris, actively utilized by government hunt operators for information collection. 	
Company: Endeavor Systems	2009 - 2010
Designation: Network Security Engineer/Developer	
<ul style="list-style-type: none"> • Built virtual infrastructure and automated environment using SDK with VMware vSphere ESX and VMware View. This includes the virtualization of desktops utilizing thin clients and developing enterprise storage solutions using Zeta File System (ZFS). 	
Company: SAIC	2009 - 2009
Designation: IOP/IA Engineer	
<ul style="list-style-type: none"> • Performed DOD-sanctioned Host Based Security System (HBSS) assessment at a major military base and built a full Air Force network security gateway test range for an Air Force Test Squadron. 	
Company: General Dynamics Advanced Information Systems	2000-2009
Designation: Network Security Engineer	
Served as incident response point man (first responder onsite) for one of computing history's most massive credit card data compromises (TJX Companies) by gathering evidence on a compromised financial asset using readily available forensics tools. Assisted in investigation by writing scripts to collect and analyze network forensic and	

log data and installing a stealthy Terminal Services session recorder on a compromised asset.	
Company: Symantec Corporation	1998-1999
Designation: Researcher	
<ul style="list-style-type: none"> Researched new security vulnerabilities on a day-to-day basis for the COTS tool. 	

3.1.6 Resume 3 – Noah Psutka

Name & Proposed Role		Education
Noah Psutka Software Developer		Texas State University May 2023 Bachelor of Science in Computer Science ➤ GPA: 3.95 / 4.00
Summary		
Results-driven Software Developer with experience in cybersecurity operations and web application development. Proficient in designing scalable applications using modern technologies such as React, Node.js, and PostgreSQL. Demonstrated ability to automate processes and enhance system efficiency through innovative solutions. Strong background in machine learning, with successful projects in face detection and exoplanet classification. Adept at collaborating within teams to deliver high-quality software solutions that meet user needs.		
Core Competencies		
<ul style="list-style-type: none"> Software Development Database Management Test Automation Machine Learning 		<ul style="list-style-type: none"> API Integration Collaboration and Teamwork Problem-Solving Front-end and Back-end Development
Technical Expertise		
<ul style="list-style-type: none"> Languages: Experience in C++, Python, Java, and JavaScript. Other Frameworks & Technologies: React, Node.js, Flask, PostgreSQL, MongoDB, Express, Linux, Git/GitHub, Agile/SCRUM 		
Employment History and Experience		
Company: Def-Logix		2024 – Present
Designation: Software Developer II		
<ul style="list-style-type: none"> Researched and developed Agentic workflows that can assist users with cybersecurity operations. Collaborated with a small team to design and develop a scalable chatbot web application using React that can serve hundreds of users and store their data within a PostgreSQL server. Integrated data pipelines to feed new information to the AI Agent to allow for more accurate responses. 		
Company: Def-Logix		2023 - 2024
Designation: Software Engineer in Test Automation		
<ul style="list-style-type: none"> Developed an application to expedite the creation of test scripts for the Test Automation team. Automated the process of forensic collection, integrating tools for a variation of operating systems. Redesigned legacy code to use REST APIs to support future development. 		
Software Projects		
Project Name: Bobcat Trail		2003 – 2023
<ul style="list-style-type: none"> Developed a web application using JavaScript that is capable of displaying an OpenStreetMap, storing user information and displaying routes with their correlated routing time and distance. Utilized REST APIs to generate pedestrian routes between buildings located at Texas State University. Achieved data persistence by implementing idb-keyval to cache user data 		
Project Name: MERN Library		2023 – 2023
<ul style="list-style-type: none"> Utilized MERN architecture to develop a webpage that interacts with a NoSQL database. Handled HTTP request methods by using Express.js and Node.js for the back-end server. Produced a dynamic client-side application by using React.js for front-end development. 		
Project Name: Computer Vision and Face Detection		2022 – 2022

- Built a machine learning model using AdaBoost to detect faces within an image.
- Achieved over 90% accuracy in face detection by training the model with thousands of classifiers.
- Preprocessed the input data of face images by cropping out extraneous data

Project Name: Exoplanet Classification Model using Machine Learning	2022 - 2022
--	-------------

- Predicted habitability of Exoplanets on the Exoplanet Catalog using Python to implement ML algorithms.
- Improved cross-validation scores by 50% through data preprocessing and supervised ML models.
- Implemented machine learning algorithms such as logistic regression, support vector machines (SVM), decision trees, and K-nearest neighbors (KNN)

3.2 Relevant Past Projects

Def-Logix has developed Crimson Raven, an AI-driven platform, and Crimson Crawler, an advanced Open-Source Intelligence (OSINT) tool, to revolutionize cybersecurity operations. At a recent Cyber Ops meetup organized and facilitated by Rob Dodson, participants engaged directly with Crimson Raven through hands-on exploration, testing its capabilities, and providing valuable feedback based on real-world experiences. This collaborative session highlighted Rob's expertise in bridging advanced technologies with user-centric facilitation, ensuring actionable insights were gathered to enhance the platform's development. Crimson Crawler complements these efforts by leveraging machine learning and data aggregation to analyze vast amounts of publicly accessible data, including social media, forums, dark web sources, and open databases, delivering deep, actionable insights into cybersecurity threats.

3.3 Background and Years in Business

Def-Logix Inc. is an 8(a) certified veteran-owned small business firm with over 15 years of experience in specialized professional services in cybersecurity, emphasizing software architecture and engineering. Through our relentless commitment to research and development, we have developed cutting-edge technologies and products that effectively address the needs of both federal and commercial clients. We have a proven track record of delivering customized software solutions for the *Department of Defense, Air Force Life Cycle Management Center (AFLMC), Department of Homeland Security (DHS), and Defense Information Systems Agency (DISA)* and developing integrated applications for government agencies' red and blue team functions. Def-Logix maintains *Level 3 Cybersecurity Maturity Model Certification (CMMC) certification*.

- Cybersecurity Research & Development
- Secure Software Design & Development
- Secure System Design
- Intrusion Detection/Prevention Systems
- Network Security Development
- Computer and Network Forensics
- Security Risk Assessment

Def-Logix Capabilities

Def-Logix's expertise in network forensics, intrusion detection/prevention, and exploit detection/prevention allows us to implement power tools that effectively detect, stop, and recover from cyber threats. We have a team of highly skilled Subject Matter Experts (SMEs) who deeply understand cybersecurity and continuously expand their knowledge base to tackle complex challenges. Focusing on delivering tailored solutions to meet our client's needs, we provide software security professionals and engineers with proven technical expertise and operational skills. Our team draws upon a comprehensive knowledge base and past performance to support commercial and government projects. We have equipped our team with various technical skills and knowledge, including system engineering, software development, network operations, cybersecurity procedures and techniques, white-hat hacker prevention methods, and zero-day prevention, ensuring our ability to deliver quality solutions for our clients.

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.

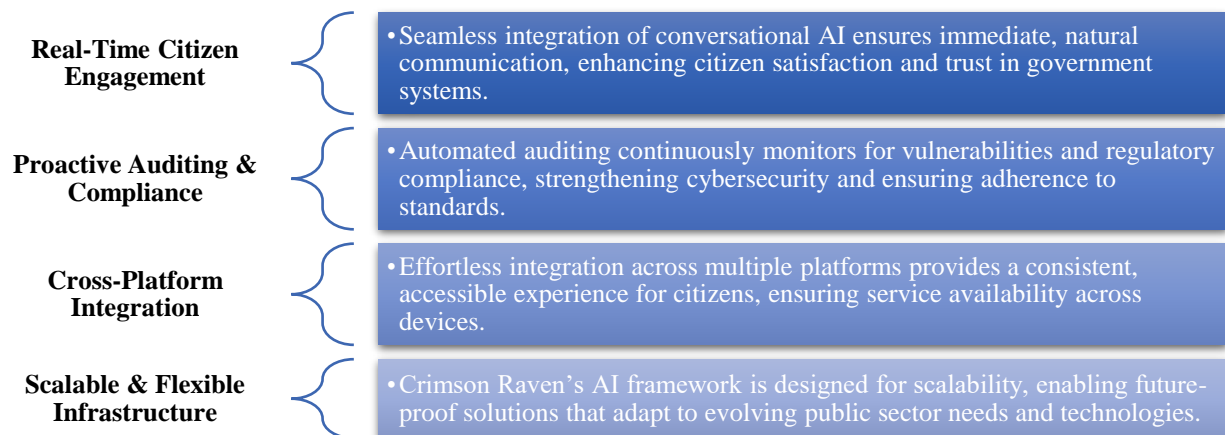


Figure 4 - Crimson Raven's AI-Driven Citizen Engagement Framework

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.

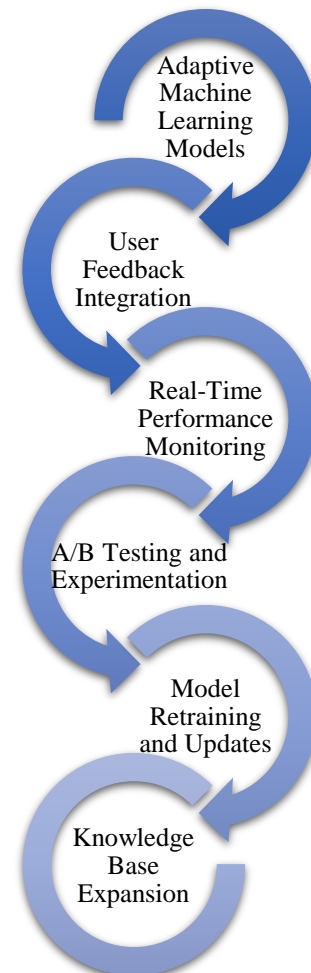


Figure 5 - Crimson Raven Continuous Improvement Framework.

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.

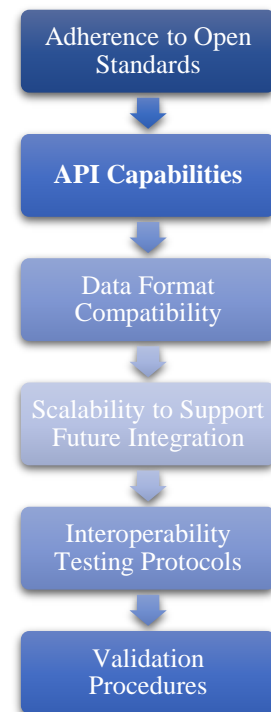


Figure 6 - Crimson Raven Interoperability Framework

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.

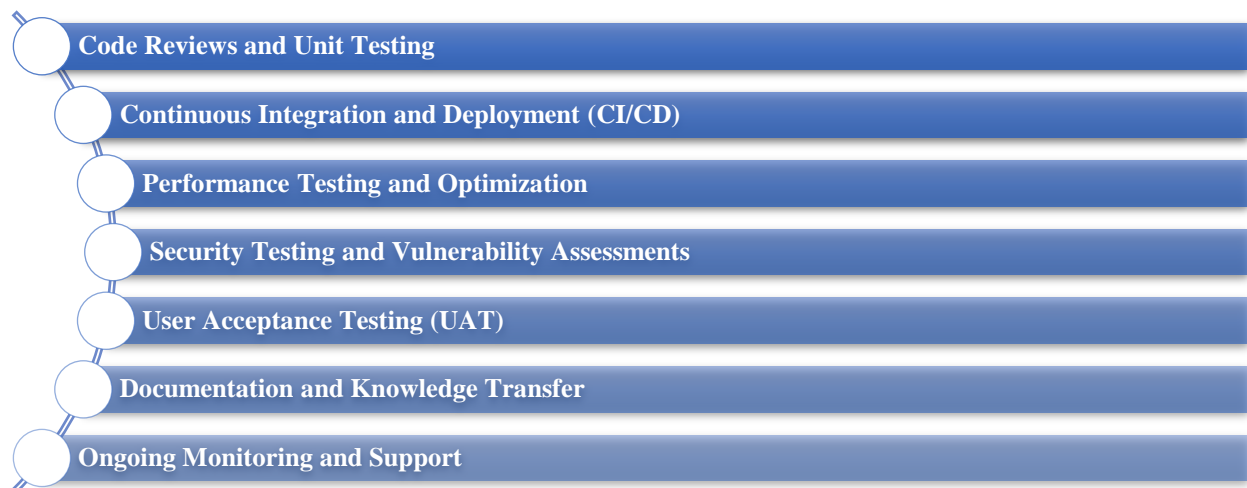


Figure 7 - Quality Control

- 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.

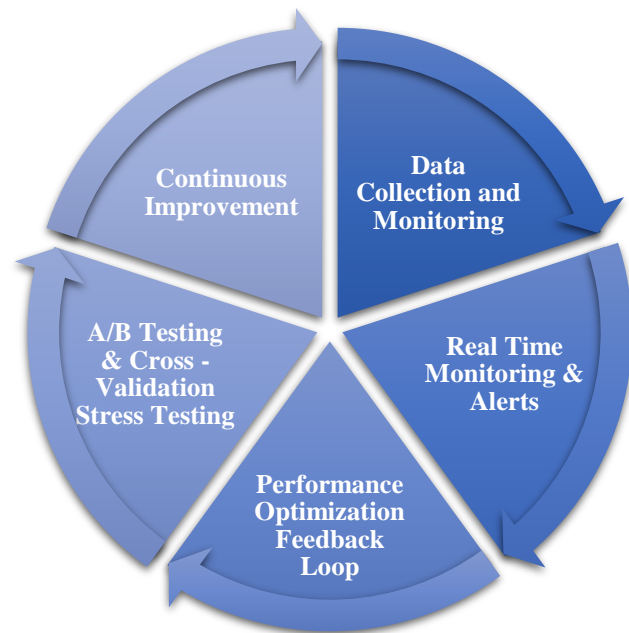


Figure 8 - Crimson Raven Performance Tracking and Feedback Loop

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

7 HUB

Texas Historically Underutilized Business (HUB) Certificate



Certificate/VID Number: **1262774089200**
Approval Date: **March 1, 2022**
Scheduled Expiration Date: **March 31, 2024**

In accordance with the Memorandum of Agreement between the
SOUTH CENTRAL TEXAS REGIONAL CERTIFICATION AGENCY (SCTRCA)
and the Texas Comptroller of Public Accounts (CPA), the CPA hereby certifies that

Def-Logix, Inc

has successfully met the established requirements of the State of Texas Historically Underutilized Business (HUB) Program to be recognized as a HUB. This certificate printed **March 1, 2022**, supersedes any registration and certificate previously issued by the HUB Program. If there are any changes regarding the information (i.e., business structure, ownership, day-to-day management, operational control, addresses, phone and fax numbers or authorized signatures) provided in the submission of the business; application for registration/certification into SCTRCA's program, you must immediately (within 30 days of such changes) notify SCTRCA's program in writing. The CPA reserves the right to conduct a compliance review at any time to confirm HUB eligibility. HUB certification may be suspended or revoked upon findings of ineligibility. If your firm ceases to remain certified in SCTRCA's program, you must apply and become certified through the State of Texas HUB program to maintain your HUB certification.

Statewide HUB Program
Statewide Procurement Division

Note: In order for State agencies and institutions of higher education (universities) to be credited for utilizing this business as a HUB, they must award payment under the Certificate/VID Number identified above. Agencies, universities and prime contractors are encouraged to verify the company's HUB certification prior to issuing a notice of award by accessing the Internet (<https://mycpa.cpa.state.tx.us/passcmblsearch/index.jsp>) or by contacting the HUB Program at **512-463-5872** or toll-free in Texas at **1-888-863-5881**.

South Central Texas Regional Certification Agency of Bexar County, Texas hereby duly affirms that:

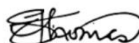
Def-Logix, Inc.

has successfully met the established requirements of SCTRCA's Business Enterprise Certification Program to be certified as a

*ESBE HABE MBE SBE VBE

Certified NAICS Codes

NAICS 541511: COMPUTER PROGRAMMING SERVICES, CUSTOM
NAICS 541512: COMPUTER SYSTEMS DESIGN SERVICES
NAICS 541513: COMPUTER FACILITIES MANAGEMENT SERVICES
NAICS 541519: OTHER COMPUTER RELATED SERVICES
NAICS 611420: COMPUTER TRAINING



Sheena Thomas
Executive Director



Certification Number: 224083716
Effective Date: August 5, 2024
Expiration Date: August 31, 2026

Note: This certificate is the property of the South Central Texas Regional Certification Agency and may be revoked should the above named firm graduate from or fails to comply with SCTRCA's Business Enterprise Program. A Certification Renewal Application is required every two years.

8 Required Attachments

Attachment I: Instructions for Proposals Compliance and Submittal

ATTACHMENT I: INSTRUCTIONS FOR PROPOSALS COMPLIANCE AND SUBMITTAL

Compliance with the Solicitation

Submissions must be in strict compliance with this solicitation. Failure to comply with all provisions of the solicitation may result in disqualification.

Compliance with the NCTCOG Standard Terms and Conditions

By signing its submission, Offeror acknowledges that it has read, understands and agrees to comply with the NCTCOG standard terms and conditions.

Acknowledgment of Insurance Requirements

By signing its submission, Offeror acknowledges that it has read and understands the insurance requirements for the submission. Offeror also understands that the evidence of required insurance must be submitted within ten (10) working days following notification of its offer being accepted; otherwise, NCTCOG may rescind its acceptance of the Offeror's proposals. The insurance requirements are outlined in Section 2.2 - General Terms and Conditions.

Name of Organization/Contractor(s):

Def-Logix, Inc.

Signature of Authorized Representative:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:54:34 -06'00'

Date: 01/13/2025

Attachment II: Certification of Offeror

ATTACHMENT II: CERTIFICATIONS OF OFFEROR

I hereby certify that the information contained in this proposal and any attachments is true and correct and may be viewed as an accurate representation of proposed services to be provided by this organization. I certify that no employee, board member, or agent of the North Central Texas Council of Governments has assisted in the preparation of this proposal. I acknowledge that I have read and understand the requirements and provisions of the solicitation and that the organization will comply with the regulations and other applicable local, state, and federal regulations and directives in the implementation of this contract.

I also certify that I have read and understood all sections of this solicitation and will comply with all the terms and conditions as stated; and furthermore that I, Paul Rivera (typed or printed name) certify that I am the CEO & Owner (title) of the corporation, partnership, or sole proprietorship, or other eligible entity named as offeror and respondent herein and that I am legally authorized to sign this offer and to submit it to the North Central Texas Council of Governments, on behalf of said offeror by authority of its governing body.

Name of Organization/Contractor(s):

Def-Logix, Inc.

Signature of Authorized Representative:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:55:22 -08'00'

Date: 01/13/2025

Attachment III: Certification Regarding Debarment

**ATTACHMENT III: CERTIFICATION
REGARDING DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS**

This certification is required by the Federal Regulations Implementing Executive Order 12549, Debarment and Suspension, 45 CFR Part 93, Government-wide Debarment and Suspension, for the Department of Agriculture (7 CFR Part 3017), Department of Labor (29 CFR Part 98), Department of Education (34 CFR Parts 85, 668, 682), Department of Health and Human Services (45 CFR Part 76).

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

1. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency;
2. Have not within a three-year period preceding this contract been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or Local) transaction or contract under a public transaction, violation of federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false Proposals, or receiving stolen property;
3. Are not presently indicated for or otherwise criminally or civilly charged by a government entity with commission of any of the offense enumerated in Paragraph (2) of this certification; and,
4. Have not within a three-year period preceding this contract had one or more public transactions terminated for cause or default.

Where the prospective recipient of federal assistance funds is unable to certify to any of the qualifications in this certification, such prospective recipient shall attach an explanation to this certification form.

Name of Organization/Contractor(s):

Def-Logix, Inc.

Signature of Authorized Representative:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:55:49 -06'00'

Date: **01/13/2025**

Attachment IV: Restrictions on Lobbying

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

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

1. No 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 officer or employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal loan, the entering into of any cooperative Contract, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative contract; and
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, and or cooperative contract, the undersigned shall complete and submit Standard Form – LLL, "Disclosure Form to Report Lobbying", in accordance with the instructions.
3. The undersigned shall require that the language of this certification be included in the award documents for all sub-awards at all tiers and that all sub-recipients shall certify accordingly.

Name of Organization/Contractor(s):

Def-Logix, Inc.

Signature of Authorized Representative:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:56:19 -06'00'

Date: 01/13/2025

Attachment V: Drug-Free Workplace Certification

ATTACHMENT V: DRUG-FREE WORKPLACE CERTIFICATION

The Def-Logix, Inc. _____ (company name) will provide a Drug Free Work Place in compliance with the Drug Free Work Place Act of 1988. The unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited on the premises of the Def-Logix, Inc. _____ (company name) or any of its facilities. Any employee who violates this prohibition will be subject to disciplinary action up to and including termination. All employees, as a condition of employment, will comply with this policy.

CERTIFICATION REGARDING DRUG-FREE WORKPLACE

This certification is required by the Federal Regulations Implementing Sections 5151-5160 of the Drug-Free Workplace Act, 41 U.S.C. 701, for the Department of Agriculture (7 CFR Part 3017), Department of Labor (29 CFR Part 98), Department of Education (34 CFR Parts 85, 668 and 682), Department of Health and Human Services (45 CFR Part 76).

The undersigned subcontractor certifies it will provide a drug-free workplace by:

Publishing a policy Proposal notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the consequences of any such action by an employee;

Establishing an ongoing drug-free awareness program to inform employees of the dangers of drug abuse in the workplace, the subcontractor's policy of maintaining a drug-free workplace, the availability of counseling, rehabilitation and employee assistance programs, and the penalties that may be imposed on employees for drug violations in the workplace;

Providing each employee with a copy of the subcontractor's policy Proposal;

Notifying the employees in the subcontractor's policy Proposal that as a condition of employment under this subcontract, employees shall abide by the terms of the policy Proposal and notifying the subcontractor in writing within five days after any conviction for a violation by the employee of a criminal drug abuse statute in the workplace;

Notifying the Board within ten (10) days of the subcontractor's receipt of a notice of a conviction of any employee; and,

Taking appropriate personnel action against an employee convicted of violating a criminal drug statute or requires such employee to participate in a drug abuse assistance or rehabilitation program.

Name of Organization/Contractor(s):

Def-Logix, Inc. _____

Signature of Authorized Representative:

Paul A. Rivera  Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:56:49 -0600

Date: 01/13/2025 _____

Attachment VI: Certification Regarding Disclosure of Conflict of Interest

**ATTACHMENT VI: DISCLOSURE OF CONFLICT OF INTEREST
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.

Name of Organization/Contractor(s):

Def-Logix, Inc.

Signature of Authorized Representative:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:57:10 -06'00'

Date: 01/13/2025

Attachment VII: Certification of Fair Business Practices

ATTACHMENT VII: CERTIFICATION OF FAIR BUSINESS PRACTICES

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.

Name of Organization/Contractor(s):

Def-Logix, Inc.

Signature of Authorized Representative:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 09:57:35 -06'00'

Date: 01/13/2025

Attachment VIII: Certification of Good Standing Texas Corporate Franchise Tax Certification

**ATTACHMENT VIII: 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 following certification that the corporation entering into this offer is current in its franchise taxes must be signed by the individual authorized on Form 2031, Corporate Board of Directors Resolution, to sign the contract for the corporation.

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.

Indicate the certification that applies to your corporation:



The Corporation is a for-profit corporation and certifies that it is not delinquent in its franchise tax payments to the State of Texas.



The Corporation is a non-profit corporation or is otherwise not subject to payment of franchise taxes to the State of Texas.

Type of Business (if not corporation):

☐

Sole Proprietor

☐

Partnership

☐

Other

Pursuant to Article 2.45, Texas Business Corporation Act, the North Central Texas Council of Governments reserves the right to request information regarding state franchise tax payments.

Paul Rivera

(Printed/Typed Name and Title of Authorized Representative)

Signature

Date: **Paul Rivera**
Digitally signed by Paul A. Rivera
Date: 2025.01.13 10:04:00 -06'00'

Attachment IX: Historically Underutilized Businesses

**ATTACHMENT IX: HISTORICALLY UNDERUTILIZED BUSINESSES,
MINORITY OR WOMEN-OWNED OR DISADVANTAGED BUSINESS ENTERPRISES**

Historically Underutilized Businesses (HUBs), minority or women-owned or disadvantaged businesses enterprises (M/W/DBE) are encouraged to participate in the solicitation process.

NCTCOG recognizes the certifications of most agencies. HUB vendors must submit a copy of their certification for consideration during the evaluation of their proposal. Please attach the copy to this form. This applies only to the Offeror and not a subcontractor.

Texas vendors who are not currently certified are encouraged to contact either the Texas United Certification Program, State of Texas HUB Program, or the North Central Texas Regional Certification Agency, among others. Contact:

State of Texas HUB Program
Texas Comptroller of Public Accounts
Lyndon B. Johnson State Office Building
111 East 17th Street
Austin, Texas 78774
(512) 463-6958
<http://www.window.state.tx.us/procurement/prog/hub/>

North Central Texas Regional Certification Agency
624 Six Flags Drive, Suite 100
Arlington, TX 76011
(817) 640-0606
<http://www.nctrca.org/certification.html>

Texas United Certification Program
USDOT website at
<https://www.transportation.gov/DBE>

You must include a copy of your certification document as part of this solicitation to receive points in the evaluation.

Vendor to Sign Below to Attest to Validity of Certification:

Def-Logix, Inc.

Vendor Name

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 10:04:49 -06'00'

Authorized Signature

Paul Rivera

Typed Name

01/13/2025

Date

☐ Not applicable.

Attachment X: Federal and State of Texas Required Procurement Provisions**ATTACHMENT X: 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.

**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.

☒ The Contractor or Subrecipient hereby certifies that it does comply with the requirements of 2 CFR §200.216 and §200.471, or applicable regulations in Public Law 115-232 Section 889.

SIGNATURE OF AUTHORIZED PERSON:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 10:05:40 -06'00'

NAME OF AUTHORIZED PERSON:

Paul Rivera

NAME OF COMPANY:

Def-Logix, Inc.

DATE:

01/13/2025

-OR-

☐ The Contractor or Subrecipient hereby certifies that it cannot comply with the requirements of 2 CFR §200.216 and §200.471, or applicable regulations in Public Law 115-232 Section 889.

SIGNATURE OF AUTHORIZED PERSON:

NAME OF AUTHORIZED PERSON:

NAME OF COMPANY:

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.

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

SIGNATURE OF AUTHORIZED PERSON:	Paul A. Rivera <div style="font-size: small; margin-top: -10px;"> Digitally signed by Paul A. Rivera Date: 2025.01.13 10:06:09 -06'00' </div>
NAME OF AUTHORIZED PERSON:	Paul Rivera
NAME OF COMPANY:	Def-Logix, Inc.
DATE:	1/13/25

-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:	_____
NAME OF AUTHORIZED PERSON:	_____
NAME OF COMPANY:	_____
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.

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

SIGNATURE OF AUTHORIZED PERSON:

Paul A. Rivera

Digitally signed by Paul A. Rivera
Date: 2025.01.13 10:06:37 -06'00'

NAME OF AUTHORIZED PERSON:

Paul Rivera

NAME OF COMPANY:

Def-Logix, Inc.

DATE:

1/13/25

-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:

NAME OF AUTHORIZED PERSON:

NAME OF COMPANY:

DATE:

Exhibit 1: Description of Desired Product Categories for Proposed Pricing

EXHIBIT 1: CATEGORIES OFFERED AND PRICING PROPOSAL

Place a checkmark next to each category you are offering in your proposal:

☒ **Service Category #1: Artificial Intelligence (AI) Solutions for Public Sector Entities**

☐ **Service Category #2: Other Ancillary Goods or Services (List Below)**

The Respondent shall furnish a comprehensive cost pricing model for this RFP, pursuant to the guidance provided in Section 5.13. Please delineate pricing based on **Service Category 1**, **Service Category 2**, or a combined pricing model for both categories. Label your pricing proposal as "Exhibit 1 – Pricing," and use as many pages as necessary to provide detailed information.

Important Note: This RFP is not tied to any specific project at this time. The purpose is to secure pricing for potential future use of AI solutions by public sector entities. Respondents are encouraged to provide pricing models that are as descriptive and flexible as possible to accommodate the varied needs of potential users.

In addition to the requested pricing, Respondents are encouraged to include a retainage rate based on the hourly rate of each staff member for any future projects that may arise but are not currently anticipated by this RFP.

Refer to Exhibit 1 –Pricing Proposal Worksheet Attachment.

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:	Indicate in the appropriate box whether you are proposing to provide service to all Fifty (50) States.		
	Will service all fifty (50) states <input checked="" type="checkbox"/>	Will not service fifty (50) states <input type="checkbox"/>	
	<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