Date: January 24th, 2025

Table of Contents

Cover Letter:

V3Main Provides IT Managed Services focusing on Cybersecurity, Custom Software Development and Cloud Computing. V3Main takes care of Clients' IT Infrastructure, Network Management and System Administration. We help our clients to migrate their legacy applications to the cloud, we manage and support them.

We also provide value added reseller services, Big Data Analytics, AI and perform POC and R&D using emerging technologies. We are a SBA 8(a) certificated company. We have GSA 8(a) STARS III Contract and Texas DIR Contract to provide Software Solutions to Texas DIR Agencies within the state including SLED, City and local Government agencies.

V3Main Technologies is your partner in technology solutions. Its strategy is to develop and deliver innovative, highly effective, yet practical approaches to the Cybersecurity, software development through robust internal processes and professionals with outstanding skills.

Our service portfolio includes custom software development, Cybersecurity, project management, content management, risk assessment, contingency planning, data warehousing, IT staffing, consulting and outsourcing.

V3Main's focus is on the integrated project management starting with project initiation through closing and transitioning into operational performance.

This proposal is in response **to TXShare ("TXS") REQUEST FOR PROPOSALS For Artificial Intelligence (AI) Solutions for Public Sector Entities ("AIS-PSE").** We recognize TXS's investment in this SFDMS. As such, we will partner with TXS to ensure our services play a vital role in supporting the AIS-PSE and the adoption of innovative technologies and management approaches.

For your consideration, V3Main has provided the enclosed information to satisfy the RFP requirements and to offer our services to perform the AIS-PSE services. This response serves as V3Main's commitment to providing the goods and services described by the TXS in the above-identified RFP.

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

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

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

V3Main agrees to and shall comply with all applicable local, state, and federal laws and regulations, as well as with all applicable Operating Policies and Procedures mandated by TXS.

Venkat Maddikayala, whose signature appears below and, on the Offer, and Submittal, is the President and CEO of V3Main Technologies, Inc. and has full authority to bind the Proposer.

01/24/2025

Sincerely,

Venkat Maddikayala, President and CEO

1 Executive Summary

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

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

2 Technical Approach

2.1 Objectives of the RFP

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

2.2 Scope of the RFP

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

2.3 Key Challenges

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

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

2.4 Current Technologies and Pain Points

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

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

2.5 Opportunities for AI Solutions

AI offers transformative opportunities to address these challenges:

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

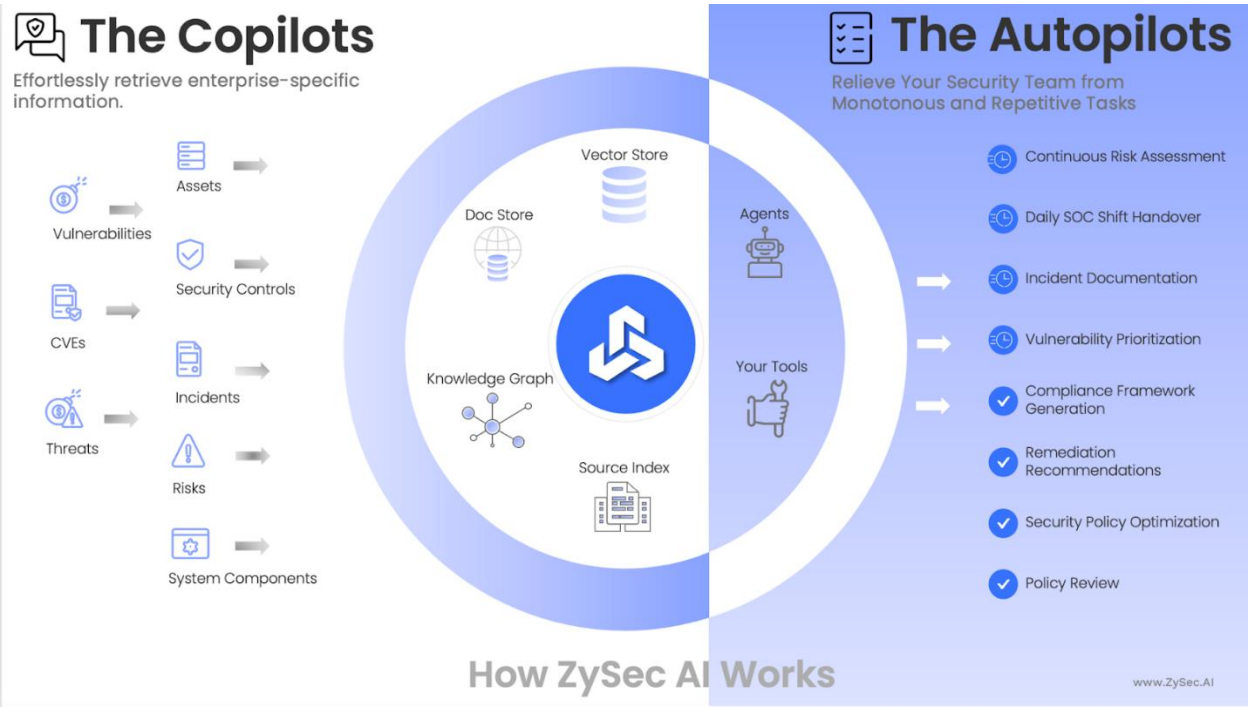
2.6 Key Considerations for the AI Solution

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

3 Introducing CyberPod AI

CyberPod AI: Autonomous Enterprise Security

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



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

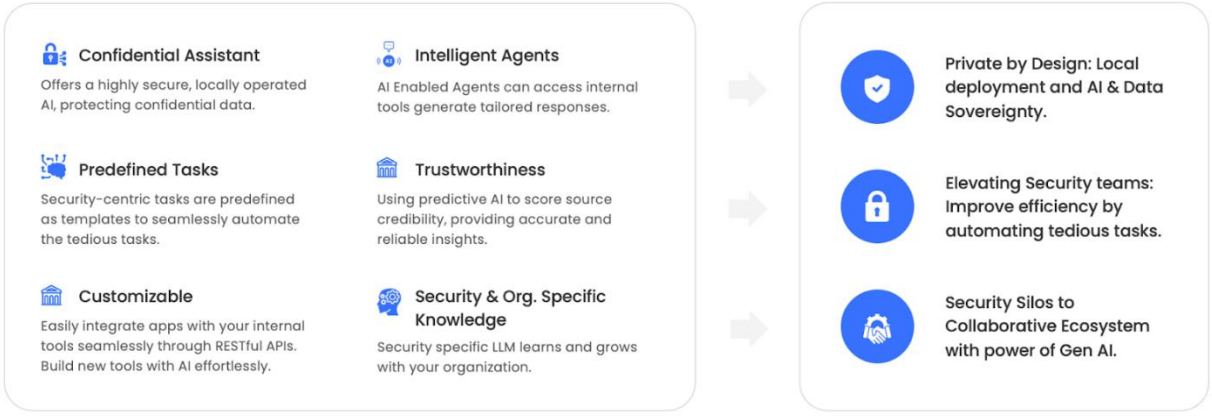
CyberPod AI leverages advanced AI to detect compliance gaps, risks, and security threats before they arise. With continuous compliance monitoring, real-time risk assessments, and adaptive governance that keeps pace with changing regulations, CyberPod AI ensures your enterprise stays secure and compliant.

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

3.1 Product Overview

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

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



Capabilities and Benefits

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

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

Use cases

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

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

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

3.2 How CyberPod AI and V3Main Experience Address Challenges:

1. **Enhanced Threat Detection and Response**:
    - CyberPod AI integrates predictive analytics with V3Main's proven threat management techniques to ensure rapid identification and neutralization of threats. This synergy optimizes security operation centers (SOCs) by automating real-time threat detection.
2. **Automation Across Security Operations**:
    - Routine tasks such as compliance documentation, vulnerability assessments, and incident reporting are automated using CyberPod's predefined templates. V3Main's domain expertise ensures these templates align with Texas government's specific requirements.
3. **Vulnerability Prioritization and Remediation**:
    - CyberPod AI's advanced risk assessment models, combined with V3Main's experience in vulnerability management for Texas government systems, streamline the prioritization and resolution of critical vulnerabilities.
4. **Seamless Integration with Existing Systems**:
    - With V3Main's deep understanding of legacy systems and CyberPod's flexible APIs, the solution integrates effortlessly with existing tools like SIEMs and firewalls, ensuring continuity and enhanced functionality.
5. **Continuous Monitoring and Risk Assessment**:
    - CyberPod AI and V3Main's monitoring frameworks provide comprehensive 24/7 oversight of critical assets. This dual approach leverages historical and real-time data to proactively identify risks.
6. **Customized Insights and Collaboration**:
    - CyberPod AI's Copilot features, supported by V3Main's insights into state-specific cybersecurity needs, enable tailored advice for different government departments. This fosters interdepartmental collaboration and informed decision-making.
7. **Data Sovereignty and Privacy**:

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

3.3 Key Differentiators

Modular, Containerized Architecture

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

Localized and Air-Gapped by Design ensures Data Sovereignty

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

Regulatory Compliance Ready

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

Specialized Cybersecurity Models

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

Effortless Usability for All Teams

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

Scalable to Organizational Needs

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

Cost-Effective Operations

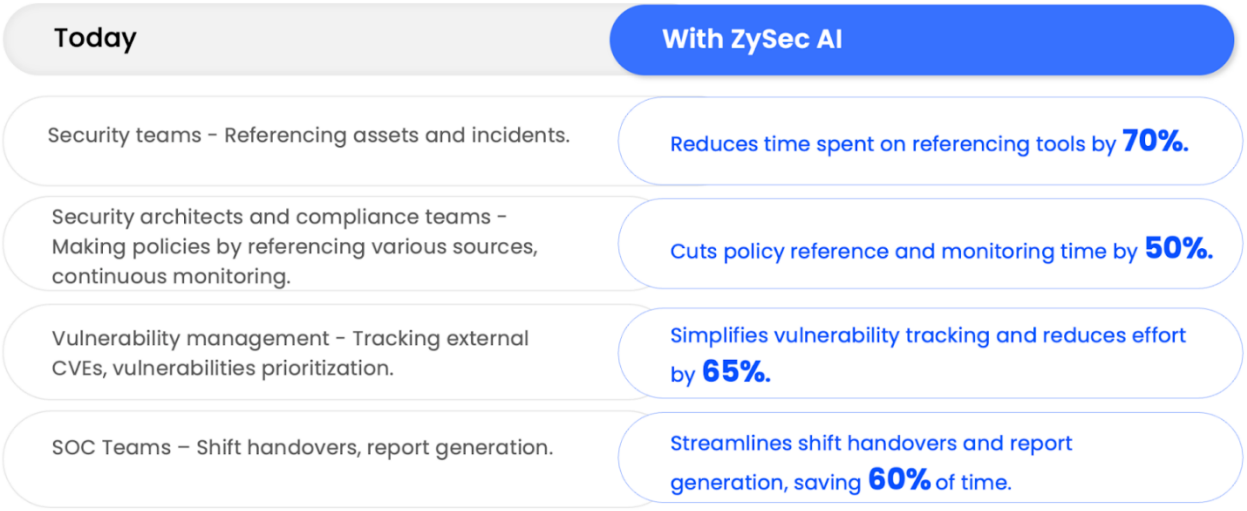
Minimizes dependency on external consultants and streamlines processes, delivering high-value outputs at significantly reduced costs.

AI-First Security Orchestration

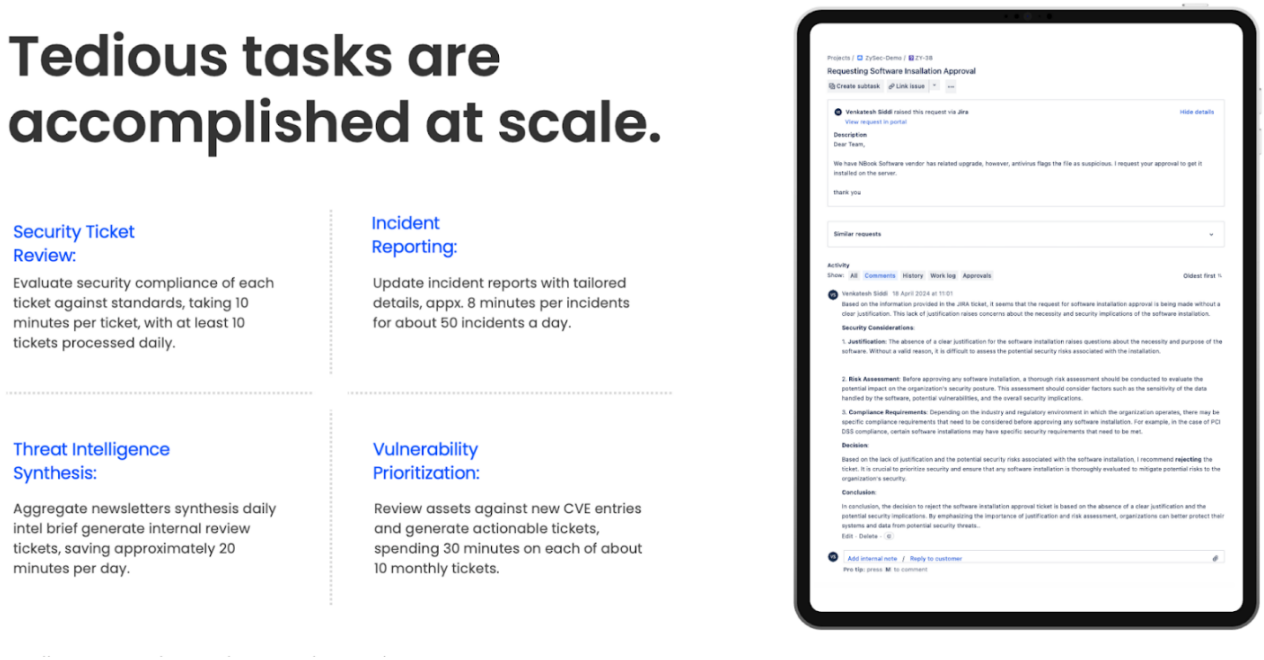
Acts as a unifying layer, connecting with existing tools to provide actionable insights and orchestrated workflows without replacing existing systems.

3.4 Organizational Impact

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



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

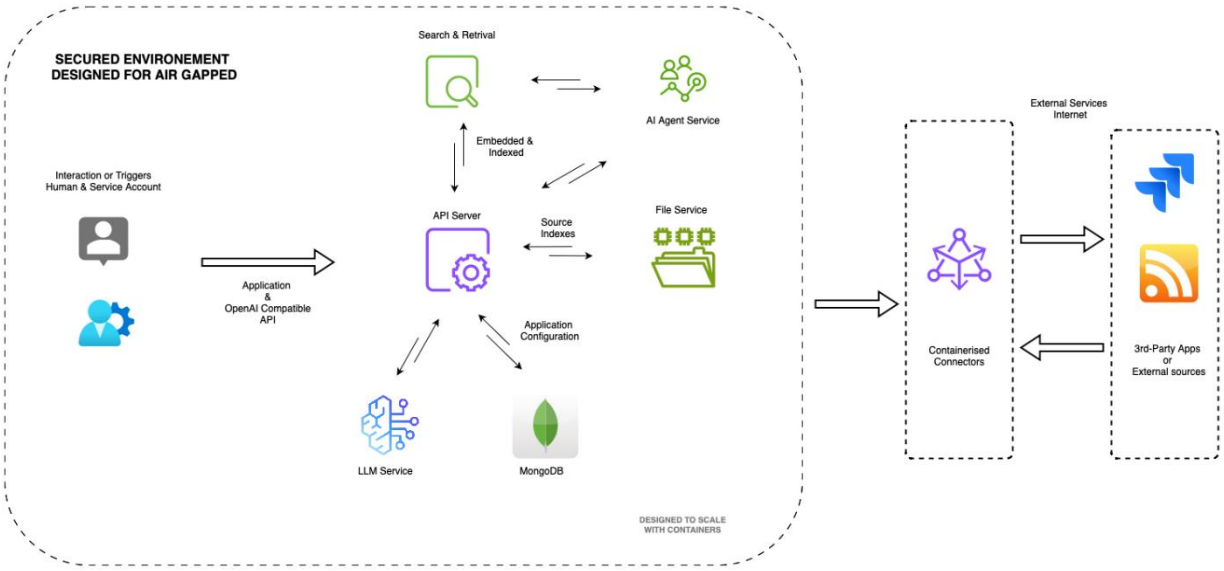


This platform empowers security teams to act with precision, make faster decisions, and focus on strategic priorities. It fosters innovation by transforming organizational security into an agile, future-ready framework capable of addressing modern challenges. CyberPod AI goes beyond incremental improvements—it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

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

4 Deployment and Integration

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



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

4.1 Solution Delivery

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

Phase 1: Requirement Analysis and Feasibility Study

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

Phase 2: Solution Design and Customization

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

Phase 3: Development and Deployment

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

Phase 4: Testing and Validation

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

Phase 5: Training, Handover, and Support

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

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

4.2 Our Experience and Credentials

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

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

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

4.3 Our Key Differentiator

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

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

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

4.4 CyperPod AI Implementation Approach

High Level Project Plan (Indicative)

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

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

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

Key Milestones and Deliverables

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

Service Governance

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

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

4.5 Key Personnel and Resume

4.5.1 Venkat Maddikayala, PMP, Enterprise Architect/Scrum Master/Contract Administrator/Project Manager

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

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

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

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

4.6 Program/Project Management

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

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

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

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

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

5 Cybersecurity Best Practices and Tools

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

5.1.1 Regular Software Updates:

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

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

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

We constantly evaluate various vendors to meet our client requirements.

5.1.2 Intrusion Detection and Prevention Systems (IDPS):

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

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

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

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

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

We constantly evaluate various vendors to meet our client requirements

5.1.3 Endpoint Protection:

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

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

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

We constantly evaluate various vendors to meet our client requirements.

5.1.4 Network Segmentation:

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

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

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

Benefits

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

Performance: Improves network performance and reduces compliance scope

Monitoring: Helps identify and fix technical issues

Isolation: Limits the spread of malware and other threats

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

We constantly evaluate various vendors to meet our client requirements.

5.1.5 Application Whitelisting:

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

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

We constantly evaluate various vendors to meet our client requirements.

5.1.6 User Education and Training:

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

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

Tools: Microsoft Phishing simulation tools, KnowBe4, Barracuda

We constantly evaluate various vendors to meet our client requirements.

5.1.7 Regular Security Assessments:

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

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

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

We constantly evaluate various vendors to meet our client requirements.

5.1.8 Backup and Recovery Plans:

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

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

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

We constantly evaluate various vendors to meet our client requirements.

5.1.9 Threat Intelligence:

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

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

We constantly evaluate various vendors to meet our client requirements.

5.1.10 Zero Trust Architecture:

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

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

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

6 Past Performance

6.1 History of the proposer

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

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

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

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

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

We experienced in delivering the below projects:

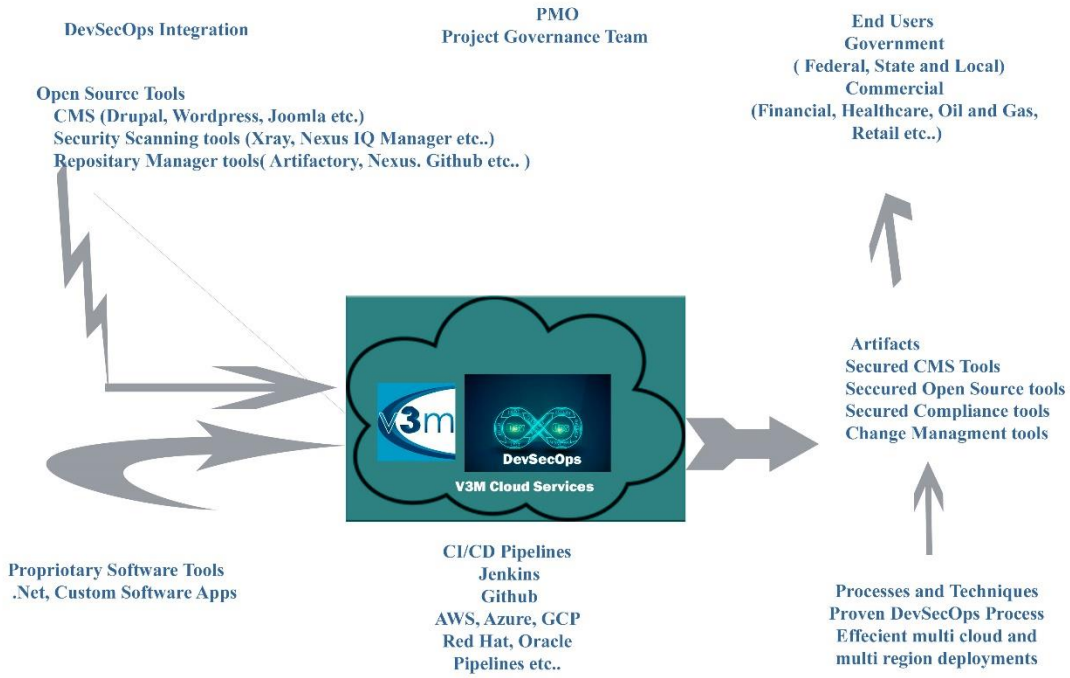
- Implement NIST Cybersecurity Framework Compliance Protect, Detect, Respond and Recover from Cybersecurity related incidents. Incident Response Planning, Threat Analysis, vulnerability management.
- Develop E-Commerce Website using .Net, Entity Framework, Content Management, Deployment, SEO, Analytics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

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

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

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

Cybersecurity and DevSecOps



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

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

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

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

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

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

6.2 Texas Comptroller of Public Accounts

Project title: Enterprise Architectural Services
Description of the project:
Enterprise IT Architectural Services including agile project management ,Infrastructure, Integration, cloud native applications development using .Net core, ESRI, and OpenShift.
Contract number: State of TX - Department of Information Resources (Enterprise Architect 2)
Scope:

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

- Addresses and resolves complex technical issues with internal/external customers, builds good communication protocols and updates management team with the weekly/monthly status.
- Perform Proof of Concepts to develop web applications using Microservices Enterprise Architecture, Micro Frontend (MFE), Backend for Frontend (BFF), and APIs
- Perform POC to replace the legacy ProMiles Application used to calculate the miles between the jurisdictions within US and Canada using ArcGIS Enterprise software, leveraging ArcGIS Network Analysis tools, Spatial Analysis tools, ArcGIS Pro 2.9, ArcGIS Enterprise Portal, ArcGIS Online portal, ArcGIS JavaScript APIs, Python APIs and .Net ArcGIS APIs and SDK, Work with the cross-functional business team to understand business problem and draw best solution.
- Re-Architect the legacy Foxpro IFTA application using modern technology using Micro Services Enterprise Architecture using ReactJs, .Net Core, OpenShift, MuleSoft, Jenkins CI/CD pipelines, JFrog, Docker and Sql Server DB
- Decompose the legacy functionality into Product backlogs, Sprint backlogs and develop Product Roadmap. Document project related documents under JIRA, Confluence, SharePoint and Bitbucket Source Code Version control system.
- Perform Data Analytics using ArcGISPro for Netowrk Analysis and Routing. Database Architectgure design for IFTA and ArcGIS Datastore

Relevance to TxShare Project:
The experience gained from the above project can be utilized as a reference architecture that can be applied to analyze the current TEXASSHARE architecture and implement necessary controls and process to improve the current operations efficiencies. The framework that was defined involves the Hybrid Cloud Infrastructure (On premise, AWS), Hyper Converged Infrastructure, Implementation of Custom Authentication and Authorization using Okta, Forgerock, Infrastructure as a Service Using Cloud Formation and Terraform, Microservices, Cloud Native Web application development using Kubernetes, and OpenShift. CI/CD using Jenkins, Vulnerabilities scanning using SonarQube, Jfrog, Checkmarx, All these projects delivered using Agile and Scrum methodology using Jira, Confluence, and Bitbucket

Point of Contacts:
Government Agency/Organization : Texas Comptroller of Public Accounts
COR's name, address, email address, and phone number:
Prime POC: Harvey Parker | Account Manager 22nd Century Technologies, Inc. I CMMi3, ISO 9001:2015 Certified ': 732-305-4531 Ext No 2054 □: http://www.tscti.com , harveyp@tscti.com

Contracting Officer's (CO's) name, organization, email address, and phone number:
Client POC: Jolly Pathak 2) Manager, Administrative Applications 3) (512) 463 2045, Jolly.pathak@cpa.texas. gov

6.3 US Navy

Project Title: DevOps Services
Description of the Project: US Navy, Naval Information Warfare Center Pacific (NIWC Pacific)
Intelligence Surveillance, Reconnaissance Dept
) Maintain, monitor, and support the infrastructure environment hosted in the Amazon Web Services (AWS) commercial cloud.

b) Maintain and optimize the automated build, test, and release CI/CD pipeline using Jenkins running as containers on AWS Elastic Compute Cloud (ECS).

c) Manage and update existing delivery processes, tools, build pipeline, configuration management and testing frameworks to include configuring, integrating open source tools, and delivering infrastructure as code (IoC).

d) Participate in iterative software development meetings and events to include daily standups, code-reviews, bi-weekly planning, sprint reviews and retrospectives as well as quarterly iterative planning sessions.

e) Support ad hoc phone calls, video, teleconferencing and emailed Q&A as required and without prior scheduling. Roughly two to three such events per week are anticipated to address ongoing technical clarification or implementation issues. The contractor shall support a 40 hour, flexible work week to accommodate system maintenance and troubleshooting, as required and without prior scheduling during non- working hours.

Contract/Order Number: Contract #NNG15SC95B. Order #N6600119F1373
Government Agency/Organization: US Navy
Current Contract/Order Status (i.e. Completed or In-Progress): Completed
Type of Contract/Order: Fixed Price
Subcontracting goal achievement, if appliable: ☒ Yes ☐ No ☐ N/A
Period of Performance, inclusive of Options: September 2019 – September 2020
Evaluator Name, Title, Email Address, and Phone Number:
POC: Angela Brown
VICTORY GLOBAL SOLUTIONS, INC.
5950 SYMPHONY WOODS RD., SUITE 211
COLUMBIA, MD 21044
PHONE: 615-708-7818 - FAX: 866-884-2726
Email: abrown@victorygs.com
Performance as Prime or Subcontractor: V3Main as a Subcontractor (Prime: Victory Global Solutions)

Relevance to TXShare:

The above experience can be leveraged implementing and supporting DevSecOps processes using AWS, Cloud Formation, AWS CI/CD processes, Auto Scaling, Upgrading the software,

Patching the application infrastructure, Network Management, Agile Project Management and Application Support activities.

6.4 Houston Calligraphy Guild

Houston Calligraphy Guild
Dates: July, 2017 - present
POC: Mimi Reilly
Title: Secretary, HCG
Phone: 713 705 2701
Email: mimi.reilly@comcast.net
Address: 3599 Westcenter Dr, Houston, TX 77042
Service: Website Redesign, Mobile App, Logo, Banners, SEO, Analytics, E-Commerce and Payments System Integration

Background:

Houston Calligraphy Guild (HCG) is a 501©3 non-profit organization founded in 1979. The current website is typepad based, unattractive and difficult to maintain since the client rely on Guild members to do this. The website is: www.houstoncalligraphyguild.org

The client HCG has decided to move the website to e weebly as a new host environment since the HCG wish to move from a blog-style website (typepad) to a WordPress theme environment with excellent security, payments and password protection capability as well as mail chimp integration.

Objectives: Attractive, clean, modern design that translates well to a mobile device environment. SSL, payments capability (for dues and courses), social media and domain-based email accounts for Houston Calligraphy Guild Officers with integrated MailChimp capability for regular member emails and notices.

Web Design Requirements:

- SSL Registration for secure communications.
- Selection of a WordPress theme **that is updated regularly for security**.
- Emails for Guild Officers tied to domain name, houstoncalligraphyguild.org and **mail chimp integration for meetings and event notices to members.**
- A secure e-commerce/shopping feature that will allow payment of dues and programs over the web.
- A password-protected “Members Only” page.
- A Gallery Page for display of member’s art work.
- Links to popular social media sites - Instagram, facebook, twitter and pinterest
- Ease of updates to web pages detailing meetings and events that would typically be done by volunteers.
- Ongoing Support and Maintenance

V3Main team has been involved in the following activities Using Agile Software Development Methodology:

1. Build a new HCG website using Weebly with Small business features
2. Build Prototype website for POC with different Themes
3. Construction of the Website based on the requirements and design documents.
4. Implement e-Commerce features and integrate with Payment Gateway Authorize.net
5. Integrate with MailChip for integration for meetings and event notices to members.
6. Resolving issues and defects reported during Acceptance Testing by Client.
7. Provide Training to the end users and documentation

Relevance to TEXASSHARE Project:

V3Main provided end to end project management, delivering the project on time, End User Support, addressing cybersecurity related incidents like phishing attack, Office 365 email support, Mobile Appl development, Support iOS and Android apps.

6.5 Houston Public Library

Houston Public Library
June 2022 – Present
Prime: V3Main Technologies
POC

ERICA LEWIS 506

832-393-1355
832-393-1438
ERICA.LEWIS@HOUSTONTX.GOV
Services: Google Licenses for Chromebooks and establish a non profit Workspace customers an community partners. COMPUTER SOFTWARE FOR MICROCOMPUTERS (PREPROGAMMED) Application Software, Microcomputer, SERVER

Relevance to TxShare Project:

Established the Google Workspace, Provisioning the Chrome OS through Zero Touch Enrollment, End User Support