RFP-12-2026
Strategic Communications
Supplier Response

Event Information

Number: RFP-12-2026
Title: Information Technology Consulting and/or Technical Services
Type: Request For Proposal
Issue Date: 3/20/2026
Deadline: 4/20/2026 02:00 PM (ET)

Contact Information

Contact: Todd Slatin
Address: Central Purchasing
Government Center Building
Room 338
200 East Main Street
Lexington, KY 40507
Phone: (859) 2583320
Fax: (859) 2583322
Email: tslatin@lexingtonky.gov

Strategic Communications Information

Contact:	Christopher Payne
Address:	310 Evergreen Road Louisville Louisville, KY 40243
Phone:	(502) 493-7234
Fax:	(502) 657-6512
Toll Free:	(502) 813-8043
Email:	cpayne@yourstrategic.com
Web Address:	www.yourstrategic.com

ONLY ONLINE BIDS WILL BE ACCEPTED! By submitting your response, you certify that you are authorized to represent and bind your company and that you agree to all bid terms and conditions as stated in the attached bid/RFP/RFQ/Quote/Auction documents.

Christopher Payne
Signature

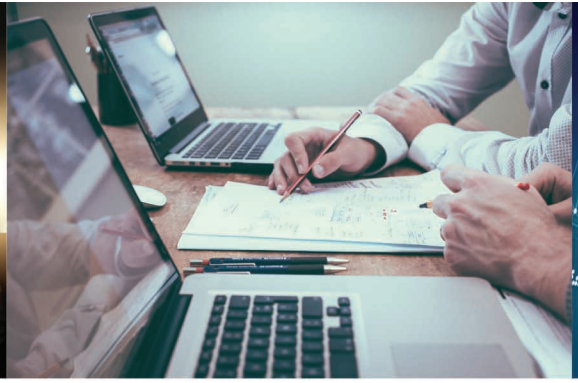
cpayne@yourstrategic.com
Email

Submitted at 4/20/2026 01:05:00 PM (ET)

Response Attachments

Lexington -Fayette IT Consulting_Strategic Communications LLC- Final.docx

Strategic Communications RFP-12-2026 Full response with documentation.

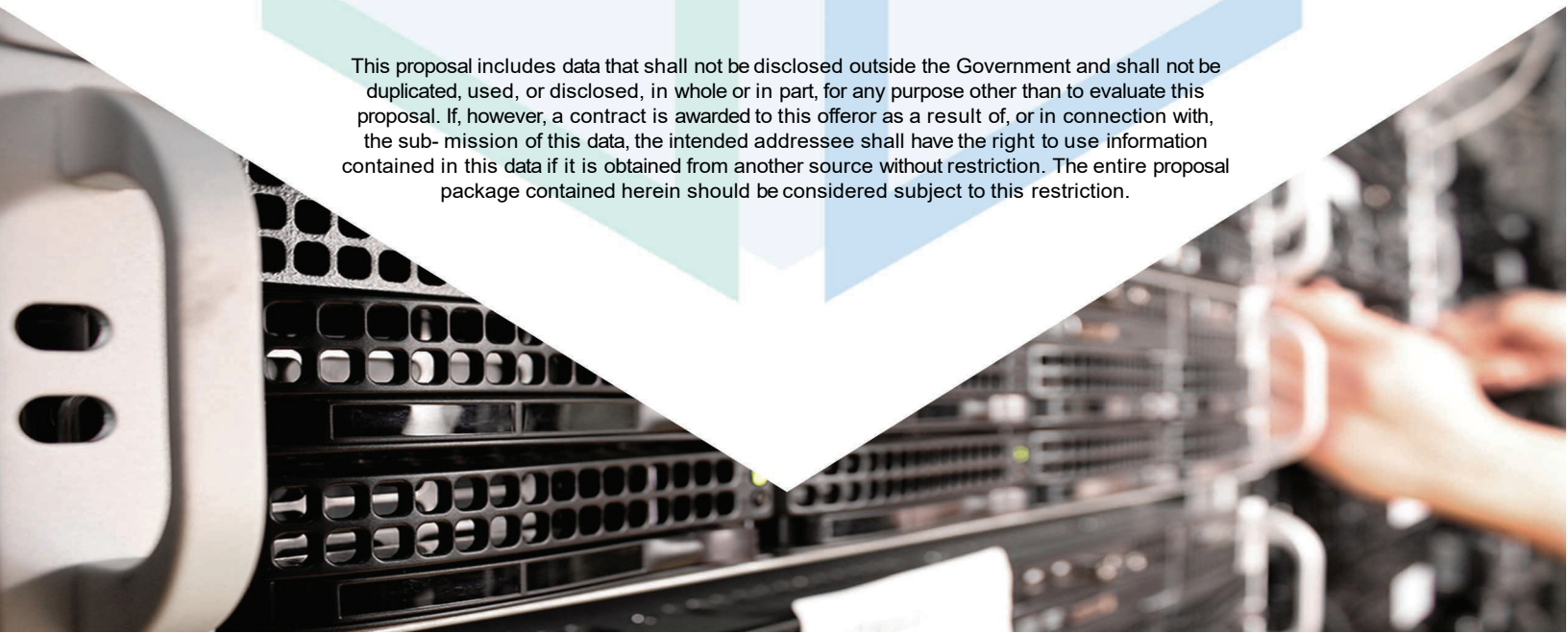

STRATEGIC COMMUNICATIONS

IT SERVICES • CLOUD • AUDIO / VIDEO

Lexington-Fayette Urban County Government Request for Proposal #12-2026 Information Technology Consulting and/or Technical Services

Submitted April 20, 2026

Strategic Communications, LLC



Contents

1. Executive Summary

Strategic Communications (Strategic), a minority woman owned small business based in Louisville, Kentucky, specializes in providing government, healthcare, education, justice, and public safety (JPS) customers with the latest in cloud, information technology (IT) and audio-visual solutions. We are public sector driven and are designed to operate as a one-stop-shop for all things multi-cloud within the public sector. Strategic is exceptionally suited to supporting the Lexington-Fayette Urban County Government. Strategic Communications brings deep expertise in consulting, design, engineering, and implementation of Information Technology (IT) solutions. This proficiency enables us to deliver customized, scalable solutions tailored to the unique needs of each client — from small agencies to enterprise-level environments.

As an authorized Federal and State Cloud Service Provider (CSP) reseller, Strategic proudly offers comprehensive cloud solutions through leading platforms including AWS, Microsoft, Google, and a portfolio of vetted solutions. These partnerships are supported by our in-house engineering and IT design teams, allowing us to combine the power of our CSP portfolios with proven architecture and deployment experience. Through this integrated partner network, we help organizations modernize infrastructure, enhance performance, recognize cost savings, and achieve secure, cloud and IT based transformations. Our depth of knowledge and Partner Alliance Community team (PAC) enables Strategic to remain agnostic when engaged with IT challenges and work towards solutions that meet the needs of a specific technical environment.

Specialized experienced and technical competence. Strategic offers:

- A dedicated public sector Cloud Sales and Technical Support team consisting of Regional Sales Directors, Customer Success Directors, Enterprise Solution Enterprise Engineers and Developers, Pre and Post Sales Support and Accounting who assist customers with their requirements. (**Exhibit 1**).
- A custom consolidated billing portal with built-in cost optimization.
- Access to all cloud regions in Amazon Web Services (AWS), Azure, and Google Cloud (GCP), including their GovClouds.
- Shared Savings through lower cost plans with no long-term commitments.
- Assistance with State legal requirements related to State purchasing mandates and compliance.
- Cloud Marketplace ready technology solutions that enable our customers to easily acquire cloud-native solutions published through multi-cloud Marketplaces, where they can be easily, and cost effectively be consumed through our existing State-level cloud contract vehicles.
- Partnerships and Approved Reseller agreements with a breadth and depth of ISVs, OEMs, the nine major technology distributors and service providers to allow the greatest competition amongst the providers.

- **Cloud Migration & Adoption -** infrastructure modernization, migration accelerator, multi-cloud adoption
- **Responsible Artificial Intelligence (AI) -** generative AI applications, secure AI framework, AI proof of concept
- **Cloud-Native App Development -** serverless app development; continuous integration and continuous delivery, Capability Maturity Model Integration (CMMI), & DevOps; application modernization
- **Advisory & Strategy -** cloud readiness assessment, CCoE implementation, professional services
- **Data Observability & Lifecycle -** data lakes/warehouses, dashboards & reporting, data migrations
- **Digital Transformation -** customer experience, business process optimization, financial optimization

Exhibit 1, Strategic offers robust capabilities in Core Cloud offerings.

Strategic has teamed with two companies in our partner network that enhance our capabilities to deliver exceptional services on this contract:

- Founded in 2004, Louisville Geek has grown from a local computer repair shop into a leading managed IT services provider supporting businesses across Kentucky and the United States. The company delivers managed services, cybersecurity, cloud solutions, co-managed IT support, and process automation through a team of engineers, project managers, and developers committed to clear communication and reliable results. The company is a privately owned, EOS run and SOC 2 compliant organization that focuses on predictable outcomes, strong partnerships, and long-term value for every client.
- FocustApps is a full-service custom software development and technology consulting firm headquartered in Louisville, Kentucky. The company specializes in designing, building, and delivering scalable, high-performance software solutions across web, mobile, cloud, and enterprise platforms. FocustApps brings deep expertise across the full software development lifecycle (SDLC), from requirements gathering and architecture design through implementation, integration, quality assurance, deployment, and ongoing support. In addition, FocustApps has a demonstrated track record of partnering with organizations across logistics, manufacturing, healthcare, field services, enterprise operations, and the public sector to solve complex technology challenges. We have direct experience working with state government agencies, most notably as the awarded vendor for the Mississippi Department of Marine Resources (MDMR) Fishing License Platform and Mobile Application, giving us firsthand familiarity with the operational, compliance, and procurement considerations that define public sector technology engagements, including data governance requirements, auditability, and the need for transparent, deliverable-based project structures.

Capacity to perform the work within the time limitations. Strategic Communications has been in business for 32 years, delivering successful technology projects nationwide. Our work spans from small $10,000 implementations to multimillion-dollar, multi-year contracts involving complex cloud architecture design and phased implementations or migrations across the United States.

We maintain established Standard Operating Procedures (SOPs) and internal Service Level Agreements (SLAs) that drive consistent project execution and quality assurance. Strategic is ISO 9001 and 9002 certified, with annual reviews conducted by independent organizations to ensure continued compliance and excellence. Our in-house engineering teams operate under defined guidelines aimed at meeting project milestones and deadlines, with the authority to redeploy resources across U.S. regions as needed to support evolving project demands.

To accelerate results, we also leverage our extensive partner community, engaging subject matter experts to meet specialized or accelerated implementation goals. Over the past 12 years, Strategic has developed, marketed, and supported the technologies specified in this solicitation—offering deep technical expertise and proven delivery experience that align with client requirements.

Past record and performance on contracts. with the Urban County government or other governmental agencies and private industry with respect to such factors as quality of work and ability to meet schedule.

Strategic Communications brings decades of experience delivering technology and communications solutions to Governmental, State, County, and Commercial clients nationwide. Our proven past performance spans three primary client sectors — State and Local, Federal, and Commercial — each built on long-term partnerships and successful project outcomes.

State & Local Government. Our State and Local team maintains statewide contracts and purchasing agreements (PAs) with Maryland, Oregon, West Virginia, New York, Connecticut, Massachusetts, Mississippi, Nebraska, and Michigan through the Oakland County G2G Marketplace. These contracts provide services (not limited to) such as Infrastructure-, Platform-, Software-, and Contact-Center-as-a-Service (IaaS, PaaS, SaaS, CCaaS) offerings, supported by extensive design and architecture experience

across major cloud service providers. Each engagement represents multi-year contracts in good standing, collectively totaling hundreds of millions of dollars in executed deliverables and serving numerous municipalities under defined contract guidelines.

Federal Government. Strategic has proudly supported federal agencies for over 30 years, providing mission-critical solutions to organizations such as HHS, CDC, DOD-DISA, SOCOM, FCC, NSF, DHA, NASA JPL and all branches of the Armed Forces — Air Force, Army, and Navy — along with civilian agencies including the U.S. Patent and Trademark Office (USPTO), IRS, and the Peace Corps. Our long-standing federal relationships demonstrate our ability to meet complex regulatory, security, and scalability requirements at the highest level.

Commercial Enterprises. In the commercial sector, Strategic maintains lasting partnerships with major enterprises including UPS, GE Aviation, LG&E/Kentucky Power, BrightSpring Health, and Goodwill, among many others. Within Kentucky, our local relationships include Boone County, Warren County, Hardin County, Jefferson County, and Louisville Metro Government. We also hold multi-year contracts with higher education institutions such as the University of Kentucky and the University of Louisville, along with technology and infrastructure work supporting K–12 entities across the Commonwealth.

Local employment. Strategic and its partners are all headquartered in Louisville, Kentucky. Our staff the majority of our staff are local and available to support the Lexington-Fayette Government as needed.

2. Vendor Requirements

2.1. Technology Assessment (Attachment A)

Strategic represents over 3,505 OEMs, cloud service providers (CSP), independent software vendors (ISV) partners and the nine major technology authorized distributors referred who provide products and deliver solutions encompassing Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Compute as a Service, Containers as a Service, Cybersecurity, JPS, Health and Human Resources solutions to name a few. Strategic's OEMs are companies like; Oracle, Red Hat, Cisco, Dell, AWS, Microsoft Azure, Adobe, Google Cloud, SearchBlox, APX, ATHD, Armour, VMware, Citrix, Dynatrace, CrowdStrike, OPSwat, Fortinet, Palo Alto and Pluralsight. Strategics' long-term relationships with our extensive partner network allow customers to rapidly acquire a plethora of customized and scalable solutions to meet increasing demands.

2.1.1. Core Infrastructure

Microsoft Windows Server (2019, 2022, and latest GA release) and Microsoft Windows 10/11 Desktop. As a 22-year-old Managed Service provider, Strategic Team has been providing support, troubleshooting, architecture, and deployment services for these systems since 2004 with almost all technical staff (85) having extensive backgrounds in both areas of technology. Currently we are responsible for the end-to-end management of 10,000 Windows desktops and over 700 Windows servers with the vast majority of these servers operating Windows Server 2019, 2022, or 2025. The use case for these servers varies wildly from domain controllers, application servers, on-premises exchange servers, hybrid exchange environments, etc.

Microsoft 365 (Architecture, Design, Security & Compliance), Microsoft Active Directory / Azure AD / Entra ID, and Microsoft Exchange Online (Cloud-first; on-prem Exchange only if required). Strategic Team is one of the leading providers of Microsoft 365 in the region and has the largest M365 portfolio of clients of any Managed Service Provider in the state. We currently have over 560 tenants under management, in which we are the primary administrator, licensing provider, and architect. A large portion of the tenants (200+) we currently have under management operate using the Entra ID, Intune, and

conditional access functionality of Entra ID to move away from the need for on-premise infrastructure. As a part of our overall management, it is expected that we will perform all management of the exchange/email services within Microsoft which is always included in our Managed Service and Microsoft service agreement. All 85 staff members are extensively trained on the functionality of Microsoft 365, Entra ID, and Exchange as they are critical applications within our client environments. We also have ten staff members who specialize in Cloud Engineering roles specifically to be escalations points for issues as well as deployment specialists for new M365 engagements.

Linux – Various modern distributions (RHEL, Ubuntu, SUSE), and Internet Information Services (IIS) (latest supported versions). Strategic Team has been the primary support, management, architectural, and deployment partner for over 800 environments across our 22 years of service working with data center operations of varying complexities. Many of our clients have been traditional ESXi customers prior to the acquisition by Broadcom and we have extensive knowledge as it relates to vSphere and vCenter management with over 30 engineers trained in the platform and ten specialized senior engineers dedicated to support and design for these environments. Linux, IIS, and F5 BIG-IP are technologies we have less regular exposure to due to the nature of them being deployed in less environments but are technologies we have worked with for over 20 years. As an organization that works within every area of technology outside of IT Audit & ERP, we also have an in-house application development team of five who have more specialized training and experience with these platforms.

2.1.2. Cloud & DevOps

Microsoft Azure Architecture & Design and Microsoft Azure IaaS / PaaS Services. Strategic Team has hands-on experience with Microsoft Azure IaaS and PaaS services across multiple production deployments. Our team regularly configures Azure App Service, Azure Functions (serverless workloads), Azure DevOps CI/CD pipelines, Azure Key Vault, Azure SQL Database, Role-based access control (RBAC), and Azure VMs as standard components of application delivery. Azure Active Directory / Entra ID integration is a routine part of our identity and access implementation practice.

Microsoft Azure DevOps (CI/CD, Pipelines). Our Teammate, Strategic Team has applied cloud and DevOps technologies as a foundational layer across multiple production engagements. Our engineers work directly within Azure and AWS environments as part of application development and data platform delivery as application-layer practitioners who depend on and configure these services to ship reliable software.

AWS Architecture & DevOps. Strategic Team engineers have applied AWS services in application hosting, database, and serverless contexts. Our experience includes Amazon RDS (MySQL, PostgreSQL, and SQL Server engines), AWS Lambda for serverless event-driven processing, S3 for object storage, and CloudWatch for monitoring and alerting. We configure Inside Account Managers (IAM) roles with least-privilege policies, apply encryption in transit and at rest as standard, and integrate AWS services into CI/CD pipelines through GitHub Actions and GitLab CI.

Infrastructure as Code (IaC). Strategic Team applies IaC practices in cloud deployments to ensure repeatable, auditable, and version-controlled infrastructure provisioning. Our teams use Terraform and Azure Bicep/ARM templates for cloud resource definition and integrate IaC steps into CI/CD pipelines so infrastructure changes follow the same review and approval gates as application code. Environment-specific variables are managed through Azure DevOps variable groups, GitHub Actions secrets, and environment-scoped deployment targets.

Containerization & Orchestration: Docker, Kubernetes (Azure Kubernetes Service (AKS)/ Elastic Kubernetes Service(EKS). CI/CD pipeline development is embedded in Strategic Team' standard engineering practice. We configure GitHub Actions and GitLab CI pipelines for automated build, test, static analysis, vulnerability scanning, Docker image builds, and environment-specific deployments on every

project. Our containerization experience includes writing multi-stage Dockerfiles, deploying containerized applications to AKS and Amazon EKS, including deployment YAML, horizontal pod autoscaling, ingress configuration, and Kubernetes RBAC. Node.js is used by our frontend and API teams as a runtime for server-side rendering, real-time WebSocket services, and build tooling within these pipelines.

2.1.3. Database & Data Platforms

Strategic Team engineers provide the full range of support to Database and Data Platforms:

- Microsoft SQL Server(2019 and latest GA release) (8 years avg,10 engineers). Strategic Team engineers have extensive hands-on experience with Microsoft SQL Server across multiple versions, including SQL Server 2019 and the current GA release. Our capabilities include relational schema design and normalization (1NF–BCNF), complex stored procedure and trigger development, index strategy and query optimization using execution plans, SQL Agent job scheduling, Always On Availability Groups for high availability, backup/restore procedures, and security configuration including row-level security and encryption at rest. We are equally proficient with SQL Server Management Studio (SSMS), Azure Data Studio, and T-SQL scripting for automation and administration.
- IBM Db2(latest supported versions) (3 years avg, 3 engineers). Strategic Team has experience working with IBM Db2 in enterprise environments where Db2 serves as the primary data persistence layer for legacy and hybrid application stacks. Our team is proficient in Db2 SQL syntax and extensions (including OLAP functions and common table expressions), schema migration from Db2 to modern platforms, query optimization using EXPLAIN and db2advis, Db2 stored procedures and user-defined functions, and integration with Java and .NET application layers via JDBC/ODBC. We have supported organizations navigating hybrid environments where Db2 coexists with newer cloud-based database services, providing data bridge and migration strategies to minimize disruption.
- Cloud Databases:Azure SQL Database,AWS RDS (7 years avg, 11 engineers). Strategic Team has direct, production-level experience deploying and managing cloud-hosted relational databases on both Microsoft Azure and AWS. On Azure, we configure Azure SQL Database instances for production SaaS applications, implement elastic pools for multi-tenant workloads, configure geo-redundancy and automated backups, and integrate Azure SQL with Azure Active Directory for identity-based access control. On AWS, our team is experienced with Amazon RDS supporting MySQL, PostgreSQL, and SQL Server engines, including parameter group tuning, Multi-availability zone (AZ) deployments, RDS Proxy for connection pooling, and CloudWatch integration for monitoring and alerting. We apply cloud database best practices including least-privilege IAM role configuration, encryption in transit and at rest, and right-sizing for cost efficiency.
- NoSQL: MongoDB,Cosmos Dataase (DB) (5 years avg, 11 engineers). Strategic Team has practical experience designing and implementing NoSQL data solutions using both MongoDB and Azure Cosmos DB. For document-oriented data models suited to dynamic or semi-structured data, mobile app backends, and real-time tracking systems. Our team applies MongoDB for flexible schema design, indexing strategies (compound, text, geospatial), aggregation pipelines for analytics, and replica set configurations for high availability. For Azure Cosmos DB, we leverage its multi-model API support (Core SQL, MongoDB-compatible API), global distribution capabilities, and seamless integration with the broader Azure ecosystem. We evaluate NoSQL vs. relational tradeoffs carefully based on access patterns, consistency requirements, and scalability needs.

The following capabilities extend beyond the four technologies listed in Attachment A but represent core Strategic Team competencies directly relevant to the data and integration needs of this engagement:

- Data Migration& ETL Pipelines. Data migration and process automation are core Strategic Team competencies. Our ETL practice covers full-lifecycle data migrations including extraction from legacy systems, schema mapping, data cleansing and transformation, validation, and load with post-migration reconciliation. We build ETL pipelines in Python (pandas, SQLAlchemy) and T-SQL, with structured error logging, rollback mechanisms, and data integrity validation throughout. For large-scale

integrations, we have applied ML-driven automation to classification and deduplication tasks, significantly reducing manual processing overhead. Our automation work has also covered OCR-based document ingestion combined with AI-assisted exception handling, eliminating high volumes of manual back-office data handling without adding headcount.

- Real-Time Data& Analytics Platforms. Strategic Team has built production systems that depend on real-time data capture, processing, and presentation. Our experience spans real-time IoT data ingestion and storage, including time-series health metrics and location tracking, through to operational analytics delivered via Power BI on top of cloud-hosted data platforms. We design real-time architectures using event-driven patterns, Azure Functions, and WebSocket services for low-latency data delivery. For analytics platforms, we implement managed BI layers with proactive monitoring, AI-enhanced pattern recognition, and self-service reporting capabilities. We evaluate real-time vs. batch processing tradeoffs based on latency requirements, data volume, and cost.
- API-Based DataIntegration. Strategic Team is highly experienced in integrating disparate data systems through RESTful and custom API connections. Our integration work spans CRM platforms, ERP systems, payment gateways, shipping carriers, marketing automation tools, and geospatial services. We design integration architectures with structured error handling, retry logic, webhook event processing, and audit logging to ensure reliability and traceability across all connected systems. API-based data integration is a cross-cutting capability applied in nearly every engagement, connecting custom-built applications to third-party platforms and enterprise systems without requiring core system replacement.

2.1.4. Application/Software Development

Application development is Strategic Team' core competency. We design and build production-grade custom software across web, mobile, enterprise, and cloud-native platforms. Our development approach is grounded in Agile methodologies, modern software engineering best practices, rigorous quality assurance (QA) and testing protocols, and a security-conscious Software Development Lifecycle (SDLC) that accounts for authentication, authorization, data encryption, and vulnerability mitigation from the earliest design stages.

We bring full-stack depth, from backend API and business logic development to responsive frontend interfaces and native mobile applications. Our team has deep experience in legacy modernization, transitioning organizations from outdated frameworks to modern, maintainable architectures without disrupting existing operations or workflows.

Core Frameworks & Runtime

- Microsoft .NET 6+ /.NET Core(modern framework) (5 years avg, 11 engineers). Strategic Team engineers are proficient with the modern .NET platform, including .NET 6, .NET 7, and .NET 8 (LTS), applied across across web APIs, background services, and enterprise application backends. We leverage .NET's cross-platform runtime capabilities to build performant, maintainable services that run on both Windows and Linux hosting environments. Our use of .NET covers dependency injection patterns, Entity Framework Core for ORM-based data access, middleware pipelines, configuration management, health checks, and structured logging via Serilog/NLog. We are experienced in migrating legacy .NET Framework applications to modern .NET, a competency that translates well to organizations modernizing legacy systems.
- ASP.NET Core(for web apps) (6 years avg, 6 engineers). ASP.NET Core is a primary web application framework for Strategic Team. We build production web applications using ASP.NET Core MVC and Razor Pages for server-rendered interfaces, as well as ASP.NET Core Web API for RESTful backend services consumed by frontend single-page applications (SPA) frameworks and mobile clients. Our ASP.NET Core work encompasses authentication and authorization (ASP.NET Core Identity, JWT bearer tokens, OAuth 2.0, OpenID Connect), model validation, error handling middleware, content negotiation, API versioning, Swagger/OpenAPI documentation generation, and deployment to IIS,

Azure App Service, and containerized environments. We apply security hardening practices including HTTPS enforcement, CSRF protection, input sanitization, and Content Security Policy headers.

- Visual Studio /Visual Studio Code (11 years avg, 13 engineers).Visual Studio (Enterprise/Professional) and Visual Studio Code are the primary IDEs used across Strategic Team' development teams. Our engineers are highly proficient with VS debugger, IntelliTrace, profiling tools, test explorer, and integrated Git workflows in Visual Studio. For cross-platform and polyglot development, we leverage VS Code extensively, with language-specific extensions, remote development containers, integrated terminal workflows, and debugging configurations for Node.js, Python, and Flutter. Our teams are also experienced with GitHub Copilot integration, live share for collaborative debugging, and workspace configuration standards that promote consistent development environments across distributed teams.

Languages

- C# (8 years avg, 12 engineers). C# is Strategic Team' primary backend programming language. Our engineers apply C# across the full spectrum of application development: ASP.NET Core web APIs and MVC applications, background worker services, console automation tools, Entity Framework Core Data access layers, unit and integration test suites (xUnit, NUnit, Moq), and Azure Functions for serverless workloads. We adhere to modern C# idioms including async/await patterns for non-blocking I/O, LINQ for expressive data queries, records and pattern matching (C# 9+), nullable reference types for safer code, and interface-based design for testability. Our C# codebases are written with long-term maintainability in mind: clean architecture principles, SOLID design, comprehensive XML documentation, and code review standards.
- Python (7 years avg, 12 engineers). Strategic Team applies Python primarily in data engineering, automation, scripting, and backend API development. Our Python capabilities include RESTful API development with FastAPI and Flask, data transformation and ETL scripting (pandas, SQLAlchemy), automation of system administration and deployment tasks, data analysis and reporting pipelines, and integration scripting for third-party API connections. Python's strength in rapid prototyping makes it valuable for initial data pipeline design before productionizing in more strongly typed environments. Our use of Python spans local scripting, cloud-hosted Lambda/Azure Function deployments, and containerized microservices. We follow PEP 8 standards, enforce type hints for maintainability, and write pytest-based test coverage for production Python services.
- JavaScript /TypeScript (12 years avg, 12 engineers). JavaScript and TypeScript are core languages for Strategic Team' frontend and Node.js development. We strongly prefer TypeScript over vanilla JavaScript in all new projects due to its type safety, improved IDE tooling, and long-term code maintainability benefits. Our TypeScript/JavaScript experience spans React component development, Angular service layers, REST and GraphQL API consumption, Node.js server-side logic, and browser extension development. We use modern ES2020+ features, module bundlers (webpack, Vite), linting (ESLint), and formatting (Prettier) as standard engineering practices. Our teams are proficient with npm/yarn dependency management and maintaining clean package.json configurations with pinned, audited dependencies.
- HTML5 / CSS3 (10 years avg, 14 engineers). Strategic Team engineers produce semantic, accessible, and responsive HTML5/CSS3 as the foundation of all web application frontends. We apply WCAG 2.1 accessibility standards, semantic element usage, and responsive design with CSS Grid and Flexbox. Our CSS practices include component-scoped styling (CSS Modules, styled-components, Tailwind CSS), CSS variables for theming, and media query strategies that ensure consistent rendering across device sizes. We work within design systems and component libraries (Material UI, Ant Design, Bootstrap) while also building fully custom design implementations from wireframes and Figma designs. Our HTML/CSS output is optimized for performance: minimal render-blocking resources, lazy loading, and Core Web Vitals compliance.

Frameworks & Libraries

- React, Angular,Vue.js (6 years avg, 12 engineers). Strategic Team builds modern, component-based SPAs using React, Angular, and Vue.js, selecting the appropriate framework based on project requirements and client environment. React is our most frequently used SPA framework; we leverage hooks (useState, useEffect, useContext, useReducer, custom hooks), React Router for client-side navigation, Redux Toolkit and Zustand for state management, and React Query for server-state synchronization. Angular is applied for enterprise-grade applications where its opinionated, full-framework architecture, including built-in dependency injection, RxJS observables, Angular Material, and the Angular CLI, which provides structural consistency at scale. Vue.js is used for projects benefiting from its gentle learning curve and flexible integration with existing HTML codebases. Across all three frameworks, we apply component-driven development, thorough unit testing (Jest, React Testing Library, Jasmine/Karma), and accessibility-first design.
- jQuery(legacy support only) (9 years avg, 11 engineers). Strategic Team engineers are proficient with jQuery and can support, maintain, and extend existing jQuery-based applications. We explicitly recognize jQuery as a legacy technology and approach engagements involving jQuery with a modernization perspective, evaluating opportunities to progressively migrate to modern JavaScript or a component framework without requiring full rewrites. Our experience with jQuery-based WordPress plugins gives us practical exposure to jQuery event handling, DOM manipulation, AJAX patterns, and plugin architecture in production environments.

APIs & Web Services : REST, GraphQL (8 years avg, 13 engineers). RESTful API design and development is a foundational capability at Strategic Team. We design APIs following REST constraints and best practices: resource-based URL design, appropriate HTTP method usage, statelessness, consistent response envelope patterns, and proper HTTP status code usage. Our REST APIs are built with ASP.NET Core Web API and Node.js and are documented using OpenAPI/Swagger for developer usability. We implement authentication via OAuth 2.0/JWT, rate limiting, API versioning, and CORS configuration as standard. We write comprehensive integration test suites for all API endpoints and apply contract testing where downstream consumers are known. For GraphQL, we apply schema definition language design, resolver implementation with DataLoader for N+1 query optimization, and Apollo Server/Client integration for scenarios where flexible, client-driven data fetching provides meaningful advantages over fixed REST endpoints.

Legacy: PHP(only for legacy systems) (5 years avg, 7 engineers). Strategic Team engineers are capable of supporting, maintaining, and extending PHP-based applications and platforms, with practical experience in WordPress plugin and theme development. We approach PHP engagements with a legacy modernization mindset, identifying opportunities to improve security posture, upgrade PHP runtime versions to currently supported releases, and introduce modern tooling (Composer, PSR standards, PHPUnit testing) where feasible. We do not initiate new greenfield development in PHP, but are fully capable partners for organizations with existing PHP-based systems requiring maintenance and enhancement.

The following capabilities extend beyond the Attachment A scope and represent additional Strategic Team strengths directly relevant to application development, modernization, and DevOps needs:

Mobile & Cross-Platform Development. React Native /Flutter(cross-platform iOS/Android). React Native is Strategic Team' primary cross-platform mobile development framework for new engagements, chosen for its strong ecosystem, native performance, and offline-first capabilities that align with how most of our clients need mobile applications to behave in the field. We have production experience with React Native across both greenfield development and complex feature implementations, including offline data synchronization, push notifications, ArcGIS map integration, and multi-channel notification delivery.Flutter is also a capability we bring to client engagements, typically in scenarios where a client has an existing Flutter codebase, a specific preference for Flutter, or where the project involves migrating from

a legacy cross-platform framework. We have led complete legacy-to-Flutter migrations, conducting comprehensive functionality assessments, rebuilding applications with clean Flutter architecture, and executing rigorous QA across iOS and Android before App Store and Google Play submissions. Our choice between React Native and Flutter is driven by the client's context and requirements rather than a blanket default.

In addition to cross-platform Flutter development, Strategic Team has native iOS development experience. We have delivered native iOS applications leveraging Apple's app lifecycle, push notification frameworks, local storage (Core Data / SQLite), offline-first data synchronization, and native networking APIs. Our iOS work includes App Store submission preparation and compliance with Apple's Human Interface Guidelines and App Review requirements. We are proficient in both Swift and the broader Apple development ecosystem, and can deliver native iOS applications for use cases where platform-level API access, performance, or App Store requirements make native development the appropriate choice.

Development Methodology & DevOps.

- Agile Scrum /Shape UpDevelopment Methodology. Strategic Team is proficient in both Agile Scrum and Shape Up methodologies, and selects or blends the approach based on what best fits the client and the nature of the engagement.Agile Scrum is well-suited for ongoing product development, teams with evolving requirements, and clients who want regular visibility into progress through sprint ceremonies. Our Agile practice includes: structured discovery and requirements phases; sprint planning with backlog grooming and story point estimation; two-week sprint cadences with daily standups and sprint reviews; continuous integration with code review gates; and formal retrospectives that drive process improvement across the engagement.Shape Up is an approach we have increasingly adopted in custom software consulting engagements, and one we find clients respond well to. It addresses a common frustration with Agile: the concern that a project will never truly finish. Shape Up works in fixed time, variable scope cycles (typically six weeks), where a problem is shaped into a well-defined pitch before any building begins, and the team has full autonomy to solve it within the cycle. There are no infinite backlogs, no sprint-to-sprint carryover, and no feature creep. Each cycle delivers something shippable. This structure tends to produce faster, more decisive outcomes for clients who want a defined scope delivered on a defined timeline, rather than an ongoing sprint cadence.We discuss methodology fit with every client during discovery, and are equally capable of delivering under either framework.
- CI/CD & Version Control(GitHub Actions, GitLab CI). Strategic Team applies modern DevOps practices across all development projects. We maintain all source code in Git repositories (GitHub and GitLab), enforcing branch protection rules, pull request review requirements, and commit message standards. CI/CD pipelines are configured using GitHub Actions and GitLab CI to automate build, test, and deployment stages, ensuring that code changes are validated through automated test suites before merging and that deployment to staging and production environments is repeatable and auditable. Our pipeline configurations include static analysis (SonarQube, ESLint), unit and integration test execution, Docker image builds, vulnerability scanning (OWASP Dependency Check, npm audit), and environment-specific deployment steps. We apply semantic versioning and maintain changelogs as part of our release management discipline.
- Containerization(Docker, Kubernetes AKS/EKS). Strategic Team engineers are proficient with Docker for application containerization and Kubernetes for container orchestration. We write multi-stage Dockerfiles that produce minimal, hardened production images, configure Docker Compose for local development parity with production environments, and deploy containerized workloads to AKS and Amazon EKS. Our Kubernetes experience covers deployment manifests, services and ingress configuration, horizontal pod autoscaling, resource limits, and RBAC. We integrate container builds and image scanning into CI/CD pipelines as standard practice, ensuring that every deployment artifact is version-controlled and auditable.
- Node.js(modern web apps). Strategic Team uses Node.js for backend API services, server-side rendering, real-time functionality (WebSocket/Socket.IO), and build tooling. Our Node.js experience

includes Express and Fastify for HTTP APIs, event-driven architecture patterns for real-time data updates, integration with third-party REST and webhook APIs, and npm ecosystem dependency management with automated audit processes. Node.js is particularly valuable in our stack for scenarios requiring high-concurrency I/O, such as real-time status update systems and webhook event processors, where its non-blocking architecture delivers superior throughput over synchronous alternatives.

Legacy Integration – Visual Basic /Desktop Application Integration. Strategic Team has hands-on experience integrating modern APIs and services into legacy desktop applications, including Visual Basic environments. We have implemented complete third-party API integrations within existing Visual Basic desktop applications, enabling automated workflows such as shipment creation, address auto-population, label generation, and real-time tracking status, without requiring end users to learn new tools or change existing workflows. This capability reflects our broader ability to bridge legacy and modern technology stacks pragmatically, delivering immediate operational value while preserving existing investments.

2.1.5. Security & Networking

Next-Gen Firewalls: Palo Alto and Network Infrastructure: Extreme Networks (wired/wireless), Routing & Switching. As a managed service provider, we are the primary network & network security management provider for 90% of our clients' environments as they do not have internal IT support capabilities to manage these technologies. Our primary "brands" in the space historically have been Cisco, Cisco Meraki, SonicWall, HPE, Fortinet, Palo Alto, Extreme Networks, with some minor exposure to Sophos & Barracuda devices among others. We have managed, deployed, and architected networks since our founding and currently have over 50 staff trained in network & network security management with 12 team members elevated to either specialty or senior engineers dedicated to network management & network security management.

Vulnerability Management: Tenable Nessus, OpenVAS, Shodan. Strategic Team embraced the concept of "Managed Security Services Provider" in 2019 due to the nature of being a managed service provider and the evolving bleed between MSSP and MSP responsibilities as well as our pre-existing responsibilities in tradition security measures including vulnerability management. We have performed vulnerability assessments using common tools like Nessus to perform these scans and coordinate efforts with our clients for management & remediation. Today we have a dedicated in-house security team who manages the majority of our security operations and our head of Cyber Operations has been with Strategic Team for 15 years and has a diverse background in datacenter, cloud, and network engineering prior to getting certified in cyber security making his perspective very useful to balance IT Operations, Business Operations, and Security Operations. Our typical approach to vulnerability management incorporates regular or persistent scanning tools and automated deployment agents to prevent repeat vulnerability remediation work allowing us to keep client environments more secure while simultaneously allowing us to focus on more critical issues by having the lower-level tasks automated.

Patch Management: Microsoft Endpoint Manager (Intune), WSUS, IBM BigFix/HCL. As an MSP, these are what we consider to be some of the primary building blocks in our contracts. Every client requires us to handle their endpoint management, endpoint support, endpoint patching, and endpoint security for all workstations and servers. We have extensive experience in using traditional MSP toolsets like RMM tools while also having a large portion of our Microsoft/Cloud forward clients operating under Microsoft native tools such as Intune & Defender which we are well versed in architecting & managing. We also have extensive experience in managing WSUS patching technology due to its existence prior to the RMM revolution in our space. Similar to the Windows Desktop & Windows Server discussion, we manage patching and endpoint security for over 10,000 workstations and 700 servers.

SIEM: Splunk, Microsoft Sentinel, managed services. After 2019, Strategic Team began working with clients to provide SIEM toolsets and SIEM management. Our current methodology is through a full

Managed Detection and Response suite that encapsulates the endpoint security, alerting, logging, and 24/7 SOC operations vs a standalone SIEM but we do work with standalone SIEM technology as well such as AlienVault, Dark Trace, and Splunk. As Microsoft partners we have an extensive background with the Microsoft Sentinel suite and have several clients who have decided to go all-in on the Microsoft security suite as their primary partner and we have supported that journey extensively. In terms of managed services, that is the primary function of Strategic Team. We are an MSP first and foremost which now includes the assumption that we will have in-house MSSP services as we do today.

Identity & Access: MFA, Conditional Access, Zero Trust Architecture. Due to the nature of our relationships with our clients and our role as their MSP/MSSP we work with almost every client to institute their conditional access policies (CAP) according to best practices or industry requirements which are always inclusive of their Multifactor Authentication policy and management. MFA has become a non-negotiable inclusion for our clients, and their CAP. Zero Trust concepts have been a growing need/desire for many businesses which we have worked extensively to assist with the implementation of many of the layers of Zero Trust. Every client has varying needs for these policies but the most common practices we have seen implemented related to network access & wireless access.

2.2. Software Development

2.2.1. Application Programming Methodology and Development Lifecycle

Strategic's Teammate, Strategic Team, is proficient in both Agile Scrum and Shape Up methodologies, and selects or blends the approach based on what best fits the client and the nature of the engagement. Every engagement begins with a thorough discovery and requirements phase, including stakeholder interviews, current-state analysis, and formal use case documentation. Development does not commence until requirements are fully defined and agreed-upon, ensuring that all work is grounded in a complete understanding of scope and acceptance criteria.

Under Agile Scrum, Strategic Team works in two-week sprints with defined goals, daily standups, sprint reviews with client stakeholders, and formal retrospectives. This approach works well for ongoing product development and clients who want regular visibility into progress. Under Shape Up, we work in fixed six-week cycles where a problem is shaped into a well-defined pitch before building begins, and the team has full autonomy to deliver something shippable within the cycle. This eliminates the open-ended backlog concern that clients often have with traditional Agile. We find Shape Up particularly well-received in custom software consulting engagements where clients want a defined scope delivered on a defined timeline. We discuss methodology fit during discovery and are equally capable of delivering under either framework.

2.2.2. Documentation Standards

Strategic Team produces and maintains comprehensive project documentation as a standard deliverable, not an afterthought. Documentation artifacts include:

- Use Case Documents: Developed at project inception and maintained through delivery, serving as the primary traceability artifact between requirements and implementation.
- Technical Architecture Documentation: System component diagrams, data flow diagrams, API specifications (OpenAPI/Swagger), and database schema documentation.
- Code Documentation: Inline XML documentation comments (C#), JSDoc (JavaScript/TypeScript), and docstrings (Python) covering all public interfaces and non-obvious logic.
- Deployment Runbooks: Step-by-step deployment instructions, environment configuration guides, and rollback procedures for production deployments.
- User Manuals & Training Materials: End-user documentation and training materials provided for all client-facing systems.

2.2.3. Secure Development Practices

Security is embedded throughout Strategic Team' SDLC rather than applied as a post-development layer. Our secure development practices are aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-53, providing a structured, risk-based approach to identifying, protecting, detecting, responding to, and recovering from security threats across all application environments. Specific practices include:

- Input validation and output encoding on all user-controlled data to prevent injection attacks (SQL injection, XSS, CSRF).
- Authentication and authorization implemented using industry-standard protocols (OAuth 2.0, OpenID Connect, JWT) with proper token lifecycle management.
- Secrets management via environment variables, Azure Key Vault, and AWS Secrets Manager. Credentials are never hardcoded in source code.
- Dependency vulnerability scanning integrated into CI/CD pipelines using OWASP Dependency Check and npm audit, with automated blocking of builds containing known critical vulnerabilities.
- HTTPS enforcement, HSTS headers, and TLS 1.2+ for all network communications.
- Principle of least-privilege applied to all service accounts, API keys, and database connection strings.
- Regular code review with security-focused review criteria as part of pull request gates.
- NIST alignment: access control and identity management aligned to NIST SP 800-53; risk assessment informed by NIST SP 800-37 (RMF); secure coding standards referenced against NIST SP 800-218 (SSDF). For government-facing engagements, Strategic Team is prepared to provide System Security Plans (SSPs), configuration baselines, and control implementation narratives consistent with NIST documentation requirements.

2.2.4. Preferred Stacks, Frameworks & Tooling

Strategic Team selects technology stacks based on project requirements, client environment, and long-term maintainability. The following reflects our preferred defaults across each layer of the stack:

- Backend / API: ASP.NET Core (C#) with .NET 8 for web APIs and microservices; Python (FastAPI or Flask) for data engineering, ETL pipelines, and automation workloads; Node.js (Express/Fastify) for high-concurrency I/O and real-time services.
- Frontend (Web): React, Angular, or Vue.js depending on project requirements; TypeScript preferred across all frameworks; Tailwind CSS or component libraries (Material UI, Ant Design); built to WCAG 2.1 AA accessibility standards.
- Mobile: React Native for cross-platform iOS/Android development; Flutter for cross-platform migration from legacy frameworks; native Swift/iOS where required.
- Data / Databases: Microsoft SQL Server and Azure SQL Database as primary relational platforms; PostgreSQL and MySQL for open-source or AWS-hosted scenarios; MongoDB and Azure Cosmos DB for document-oriented or multi-model workloads; Power BI for analytics and reporting layers.
- Cloud Infrastructure: Microsoft Azure as primary cloud platform; AWS as secondary platform. Infrastructure provisioned via Terraform and Azure Bicep/ARM templates (IaC-first approach).
- DevOps & CI/CD: GitHub Actions and GitLab CI for pipeline automation; Docker for containerization; Kubernetes (AKS/EKS) for orchestration; OWASP Dependency Check and npm audit for vulnerability scanning; semantic versioning with protected release branches.
- Security Tooling: Azure Key Vault and AWS Secrets Manager for secrets management; Microsoft Entra ID for identity and access management; HTTPS/TLS 1.2+ enforced on all endpoints; OWASP Dependency Check for application security scanning; OpenAPI/Swagger for API contract documentation.
- Project & Documentation: Linear for sprint management and backlog tracking; GitHub/GitLab for source control; Google Workspace and Slack (with integrations) for documentation and team collaboration; OpenAPI/Swagger for API specs; Figma for UI/UX design handoff.

2.2.5. Quality Assurance & Testing

Strategic Team maintains dedicated QA Engineers on staff, professionals whose sole focus is quality assurance and test execution, independent of the development team. This separation of QA responsibilities ensures objective, thorough validation of every deliverable without the blind spots that can emerge when developers test their own code. Our QA Engineers are embedded in every project sprint from the requirements phase forward, writing test plans and acceptance criteria before development begins and executing structured test cycles throughout. Our multi-stage QA process includes functional testing against defined use cases, regression testing across affected application areas, cross-platform and cross-browser compatibility testing, performance testing for high-load scenarios, exploratory testing to surface edge cases, and formal UAT with client stakeholders prior to production release. Defects are tracked, prioritized, and resolved within sprint cycles, with test results documented and available to clients as part of project closeout deliverables.

2.3. Consulting Services (Attachment B)

Strategic offers comprehensive cloud consulting services. We work closely with State agencies to assess their current infrastructure, identify areas for optimization, and develop tailored cloud strategies that align with Kentucky's goals and compliance requirements. We bring specialized knowledge of AWS, Azure, Google Cloud, and Oracle, ensuring Kentucky has access to expert advice for its specific cloud needs.

- AWS Consulting Services: Strategic provides guidance on migrating existing workloads to AWS, designing cloud architectures, and optimizing cloud usage for cost efficiency and scalability.
- Azure Expertise: With deep knowledge of Microsoft Azure's hybrid capabilities and integration with legacy systems, we ensure Kentucky can leverage Azure to meet its unique requirements, whether for application modernization or hybrid cloud deployment.
- Google Cloud and Oracle Consulting: For State agencies focused on data analytics, ML, or enterprise database management, we provide tailored services for building scalable, secure solutions on Google Cloud and Oracle Cloud Infrastructure (OCI).

For example, for the State of Maryland, Strategic's engineering team and our partner AWS provides consulting and advisory services to thew State of Maryland (SOM), advising them in the creation of security controls to comply with the published SOM IT Security Manual, moderate level security requirements. These services include defining the organizational and system scope, identify and interview system owners, regulatory factors, sensitive information storage and evaluation of AWS Cloud environments to meet or exceed security compliance requirements. Our team also assists SOM in identifying high risks areas and security compliance gaps, perform system test to validate the implementation of controls as applicable and provide code or templates to remediate non-compliant controls reported in the external audit reports.

Another example is the National Science Foundation, where Strategic helped the National Science Foundation (NSF) orchestrate an advanced, centralized management strategy for its diverse cloud infrastructure across AWS, Microsoft Azure, and GCP. By leveraging the capabilities of AWS Organizations for AWS services, Azure Management Groups for Azure services, and Google Cloud Folders for GCP services, our support facilitated the meticulous organization, grouping, and policy application across multiple accounts, subscriptions, and projects in alignment with NSF's specific business and security needs. This strategic approach significantly enhanced NSF's operational agility enforced consistent security and governance policies across its cloud environments, and eliminated the reliance on labor-intensive, manual processes and custom scripting to ensure a seamless, secure, and efficient cloud management experience that supports NSF's mission-critical operations and research initiatives.

2.3.1. Software Development

Software development is Strategic Team' primary service offering. We design, build, and deliver production-grade custom applications across web, mobile, enterprise, and cloud-native platforms. Our full-stack team spans frontend, backend, API, mobile, and DevOps disciplines, delivering end-to-end solutions from requirements through deployment and ongoing support.

Our development practice is grounded in either Agile Scrum or Shape Up methodology depending on client fit, a security-conscious SDLC aligned with NIST SP 800-218 (Secure Software Development Framework), and a dedicated QA engineering function that is independent from the development team. Every engagement includes comprehensive use case documentation, structured delivery cycles, rigorous multi-stage testing, and formal knowledge transfer at closeout. Our expertise includes:

- ASP.NET Core (C#) (6 years avg, 6 engineers). ASP.NET Core is a primary web application framework for Strategic Team. We build production web applications using ASP.NET Core MVC and Razor Pages for server-rendered interfaces, as well as ASP.NET Core Web API for RESTful backend services consumed by frontend SPA frameworks and mobile clients. Our ASP.NET Core work encompasses authentication and authorization (ASP.NET Core Identity, JWT bearer tokens, OAuth 2.0, OpenID Connect), model validation, error handling middleware, content negotiation, API versioning, Swagger/OpenAPI documentation generation, and deployment to IIS, Azure App Service, and containerized environments. We apply security hardening practices including HTTPS enforcement, CSRF protection, input sanitization, and Content Security Policy headers.
- JavaScript /TypeScript (12 years avg , 12 engineers). JavaScript and TypeScript are core languages for Strategic Team' frontend and Node.js development. We strongly prefer TypeScript over vanilla JavaScript in all new projects due to its type safety, improved IDE tooling, and long-term code maintainability benefits. Our TypeScript/JavaScript experience spans React component development, Angular service layers, REST and GraphQL API consumption, Node.js server-side logic, and browser extension development. We use modern ES2020+ features, module bundlers (webpack, Vite), linting (ESLint), and formatting (Prettier) as standard engineering practices. Our teams are proficient with npm/yarn dependency management and maintaining clean package.json configurations with pinned, audited dependencies.
- Python (7 years avg, 12 engineers). Strategic Team applies Python primarily in data engineering, automation, scripting, and backend API development. Our Python capabilities include RESTful API development with FastAPI and Flask, data transformation and ETL scripting (pandas, SQLAlchemy), automation of system administration and deployment tasks, data analysis and reporting pipelines, and integration scripting for third-party API connections. Python's strength in rapid prototyping makes it valuable for initial data pipeline design before productionizing in more strongly typed environments. Our use of Python spans local scripting, cloud-hosted Lambda/Azure Function deployments, and containerized microservices. We follow PEP 8 standards, enforce type hints for maintainability, and write pytest-based test coverage for production Python services.
- HTML5 / CSS3 (10 years avg, 14 engineers). Strategic Team engineers produce semantic, accessible, and responsive HTML5/CSS3 as the foundation of all web application frontends. We apply WCAG 2.1 accessibility standards, semantic element usage, and responsive design with CSS Grid and Flexbox. Our CSS practices include component-scoped styling (CSS Modules, styled-components, Tailwind CSS), CSS variables for theming, and media query strategies that ensure consistent rendering across device sizes. We work within design systems and component libraries (Material UI, Ant Design, Bootstrap) while also building fully custom design implementations from wireframes and Figma designs. Our HTML/CSS output is optimized for performance: minimal render-blocking resources, lazy loading, and Core Web Vitals compliance.
- Modern Frameworks:React, Angular, Vue.js (6 years avg, 12 engineers). Strategic Team builds modern, component-based SPAs using React, Angular, and Vue.js, selecting the appropriate framework based on project requirements and client environment. React is our most frequently used SPA framework; we

leverage hooks (useState, useEffect, useContext, useReducer, custom hooks), React Router for client-side navigation, Redux Toolkit and Zustand for state management, and React Query for server-state synchronization. Angular is applied for enterprise-grade applications where its opinionated, full-framework architecture, including built-in dependency injection, RxJS observables, Angular Material, and the Angular CLI, which provides structural consistency at scale. Vue.js is used for projects benefiting from its gentle learning curve and flexible integration with existing HTML codebases. Across all three frameworks, we apply component-driven development, thorough unit testing (Jest, React Testing Library, Jasmine/Karma), and accessibility-first design.

- RESTful & GraphQLAPI Development (8 years avg, 13 engineers). RESTful and GraphQL API development is a foundational service offering at Strategic Team. We design, build, document, and maintain production APIs that serve as the integration backbone for web applications, mobile clients, third-party systems, and enterprise platforms. Our RESTful API practice follows REST architectural constraints: resource-based URL design, proper HTTP method usage, stateless request/response cycles, consistent JSON response envelopes, and appropriate HTTP status codes. APIs are documented using OpenAPI/Swagger specifications, enabling clear contracts between producers and consumers. GraphQL is applied where client-driven data fetching, hierarchical data models, or multi-source data aggregation deliver meaningful advantages over fixed REST endpoints. We implement authentication via OAuth 2.0, OpenID Connect, and JWT bearer tokens; rate limiting and throttling for public-facing APIs; API versioning strategies that protect existing consumers; and CORS configuration for browser-based clients. Production examples include the FedEx API integration for PaperCone, the HubSpot CRM integration for Total Fleet Solutions, the Salesforce Marketing Cloud integration for OnPoint Group, and the PowerHive Return on Investment (ROI) calculator. All APIs include comprehensive integration test suites, structured error handling, and are deployed behind HTTPS with TLS 1.2+ enforcement.

2.3.2. Database Design & Data Services

Strategic Team brings comprehensive capabilities across relational, cloud, and NoSQL database platforms. Our engineers design, implement, optimize, and maintain database architectures that underpin mission-critical applications. We approach every data layer engagement with a focus on data integrity, performance tuning, security, scalability, and long-term maintainability across the full database lifecycle: schema design and normalization, stored procedures and triggers, indexing and query optimization, ETL/data pipeline development, cloud migration, backup and recovery planning, and real-time data access for application integrations. Our services include:

- Microsoft SQL Server (8 years avg, 10 engineers). Strategic Team engineers have extensive hands-on experience with Microsoft SQL Server across multiple versions, including SQL Server 2019 and the current GA release. Our capabilities include relational schema design and normalization (1NF–BCNF), complex stored procedure and trigger development, index strategy and query optimization using execution plans, SQL Agent job scheduling, Always On Availability Groups for high availability, backup/restore procedures, and security configuration including row-level security and encryption at rest. We are equally proficient with SSMS, Azure Data Studio, and T-SQL scripting for automation and administration.
- Azure SQL Database (7 years avg, 11 engineers). Strategic Team has direct, production-level experience with Azure SQL Database as a managed cloud relational database service. Our capabilities include configuring Azure SQL instances for production SaaS applications, implementing elastic pools for multi-tenant workloads, configuring geo-redundant backups and point-in-time restore, integrating Azure SQL with Azure Active Directory for identity-based access control, and tuning performance through Query Performance Insight and index advisor recommendations. We have applied Azure SQL in governed data architectures supporting ingestion-level validation, deduplication pipelines, and event-driven refresh cycles across complex multi-system environments.
- MySQL / PostgreSQL (7 years avg, 11 engineers). Strategic Team engineers have hands-on experience with both MySQL and PostgreSQL as open-source relational database platforms, applied across

application development, cloud hosting, and data migration engagements. On the PostgreSQL side, our experience includes schema design, advanced indexing (B-tree, GIN for full-text search, partial indexes), stored procedures and triggers, JSONB columns for semi-structured data, and connection management via PgBouncer. MySQL expertise covers InnoDB engine configuration, query optimization using EXPLAIN plans, replication setup for read scaling, and migration tooling. Both platforms are regularly deployed via Amazon RDS in our cloud engagements, where we configure parameter groups, Multi-AZ deployments for high availability, automated backups, and CloudWatch monitoring.

- Oracle Database. Strategic Team has working familiarity with Oracle Database in the context of application integration and data migration engagements. While Oracle administration and DBA services are not a primary Strategic Team offering, our development teams are proficient in Oracle SQL and PL/SQL for application-layer interactions, including complex queries, stored procedure consumption, and JDBC/ODP.NET connectivity from .NET and Java application stacks. For LFUCG engagements involving Oracle-hosted data, Strategic Team is a capable integration and application development partner.
- NoSQL(MongoDB,Cosmos DB) (5 years avg, 11 engineers). Strategic Team has practical experience designing and implementing NoSQL data solutions using both MongoDB and Azure Cosmos DB. For document-oriented data models suited to dynamic or semi-structured data, mobile app backends, and real-time tracking systems. Our team applies MongoDB for flexible schema design, indexing strategies (compound, text, geospatial), aggregation pipelines for analytics, and replica set configurations for high availability. For Azure Cosmos DB, we leverage its multi-model API support (Core SQL, MongoDB-compatible API), global distribution capabilities, and seamless integration with the broader Azure ecosystem. We evaluate NoSQL vs. relational tradeoffs carefully based on access patterns, consistency requirements, and scalability needs.

2.3.3. Consulting Services

Disaster Recovery (DR) & Business Continuity Planning. Strategic recognizes that even with highly resilient cloud infrastructure, certain inherent DR risks exist across cloud and hybrid environments. These risks vary by deployment model, geographic configuration, data classification, and customer-specific business continuity requirements.

Strategics' inherent Common DR Risks and Mitigation Strategies are provided in Exhibit 2.Strategic partners with leading cloud OEMs and Partner Alliance Community (PAC) providers to implement best-practice architectures that meet Federal Information Security Management Act (FISMA), NIST SP 800-53, and the Federal Risk and Authorization Management Program (FedRAMP)/GOVRAMP Moderate DR standards. These designs are tailored to each agency's mission needs, SLAs, and data sensitivity levels.

Risk	Description	Mitigation Strategy
Single-Region Architecture	Deploying workloads in only one cloud region increases exposure to regional outages due to natural disasters, service disruptions, or geopolitical risks.	Strategic encourages the use of multi-region deployments in AWS (e.g., active-active or active-passive between GovCloud East and West) to ensure high availability and regional failover capabilities.
Insufficient Backup Testing	Backups may exist, but without regular validation, they may be corrupted, misconfigured, or outdated.	Strategic implements automated backup validation using AWS Backup Vault Lock, backup lifecycle policies, and periodic test restorations in isolated environments.
Dependency on a Single-AZ	Deploying services in a single-AZ risks complete application failure if that zone experiences a disruption.	We enforce the use of Multi-AZ deployments for compute, database, and storage services (e.g., Amazon RDS Multi-AZ, EC2 with load balancers) to ensure zone-level fault tolerance.
Human Error in Failover Execution	Manual intervention during a disaster can lead to delayed or incorrect recovery steps.	Strategic uses IaC (e.g., AWS CloudFormation or Terraform) to define repeatable, automated failover

Risk	Description	Mitigation Strategy
		workflows, and runbooks maintained through version control and pre-approved SOPs.
Latency or Cost Impacts of Cross-Region DR	While multi-region DR improves resilience, it may introduce latency and increased replication costs for data.	We assess workload criticality and data sensitivity to apply tiered DR strategies, balancing nearline vs. cold standby solutions (e.g., S3 Standard vs. Glacier Deep Archive) based on RTO/Recovery Point Objective (RPO) requirements.

Exhibit 2: DR Risks and Mitigation Strategies.

Strategic maintains a comprehensive security, resilience, and DR framework for all cloud and IT services provided. We deliver this framework through our internal expertise and a network of best-in-class Fulfillment Partner, Subcontractor or third-party Provider Partners encompassing OEMs, including AWS, Microsoft Azure, Rackspace, Veeam, and Arctic Wolf. This ensures Participating Entities benefit from federated contingency planning, automated failover capabilities, and contractually enforced service level commitments.

Strategics' cloud provides multiple redundancy options. The systems automatically failover to secondary datacenter to prevent extended downtime. In the event of extended downtime affecting a customer's cloud workload or service:

- Initial Triage: Strategic activates its IR Protocol and assigns an Incident Manager from our Program Office to coordinate response efforts.
- Root Cause Analysis: Immediate diagnostic reviews are conducted with the impacted CSP (e.g., AWS, Azure) to isolate infrastructure, application, or network-related root causes.
- Failover Activation: When architected for high availability, impacted workloads are automatically or manually redirected to a redundant region or AZ, as defined in the customer's continuity plan.
- Customer Communication: Strategic provides hourly updates to the affected customer's designated contacts, including estimated time to resolution and business impact statements.

In addition, Strategics' providers have the infrastructure and processes in place to protect against data loss. In addition, customers may institute routine data backups using third-party apps. See Strategics' responses in Section III.O and III.U for additional information. In the rare event of data corruption or unrecoverable loss:

- Backup Validation: Strategic ensures that all cloud-deployed systems include regular, validated backups, scheduled according to the client's RPO.
- Immutable Backup Storage: For sensitive workloads, we utilize air-gapped or Write-Once-Read-Many storage policies (e.g., AWS Backup Vault Lock, Veeam Immutability) to protect against tampering or ransomware.
- Data Restoration: If data loss occurs, Strategic initiates the restoration process from the last known good backup in accordance with pre-defined recovery protocols.
- Forensic Review: A joint Strategic/Partner investigation is conducted to confirm data integrity and root cause, with audit records preserved for regulatory reporting.

Strategics' providers have infrastructure and processes in place to protect against system failure. See Strategics' response in III.U for additional information. If Strategic experiences a core system failure affecting our service delivery systems (e.g., support portals, billing systems, monitoring platforms):

- Failover to Secondary Systems: Core internal systems are hosted in a redundant cloud architecture with hot-standby or warm-failover infrastructure enabled.
- Customer Access Maintained: All critical customer-facing functions (e.g., ticketing, support intake, Service Level Agreements (SLA) reporting) are accessible via our alternate systems or through partner portals.

- Escalation to Executive Command Team: Strategics' executive incident command team convenes within 30 minutes of any internal outage and remains engaged until full restoration.
- Customer Impact Mitigation: If any delay to customer-facing deliverables is anticipated, contingency staffing plans are activated to ensure continuity.

Technical Requirements Gathering. Technical requirements gathering is embedded in our project initiation process on every engagement. We conduct structured stakeholder interviews, current-state analysis sessions, and facilitated workshops to elicit, document, and validate requirements before development begins. Deliverables include formal use case documents, functional specifications, acceptance criteria, and traceability matrices that link requirements to implementation. For LFUCG, this means every engagement begins with a clear, documented, mutually agreed-upon scope that protects the government's investment and provides measurable criteria for delivery acceptance.

IT Strategic Planning & Roadmaps. Strategic provides pre-sales planning support process that empowers our customers to make informed and strategic decisions for cloud services:

- Market Research. As part of our commitment to delivering the most relevant and actionable insights, Strategic leverages our technology partners along with our partnerships with industry-leading research organizations such as GovSpend, e. Republic, Gartner, and Forrester. These partnerships provide us with access to real-time data, market forecasts, and trend analysis, allowing data-driven decisions based on the latest research and market conditions. This research enables our customers to assess its options across multiple cloud providers and third-party vendors without limiting competition.
- Needs Assessments. Strategic collaborates with our end users to conduct in-depth needs assessments. These assessments are designed to ensure each agency's specific technical, operational, and security needs are thoroughly understood before moving into the procurement process. We engage key stakeholders to understand their current and future requirements, ensuring our assessments are both comprehensive and forward-looking. Based on the needs identified, we provide custom recommendations that are vendor-neutral and focused on achieving the best possible outcomes without limiting the scope of future solicitations.
- Cost Forecasting. Strategic also provides preliminary cost forecasting to provide a clear understanding of potential costs across different cloud platforms. This includes forecasting the total cost of ownership for AWS, Microsoft Azure, Google Cloud, and Oracle, as well as evaluating third-party services.

Our Technology Project Manager (PM) combines technical knowledge with business acumen and soft skills. They oversee planning along with day-to-day project delivery activities while managing relationships with diverse teams to achieve the desired technical implementations. The TAM:

- Engages during pre-sales for complex, non-product-only solutions.
- Provides technical insight, architecture design, and solution validation.
- Continues advisory role post-sale if needed for deeper technical alignment.

We engage an Enterprise PM from the Project Management Office (PMO) Team)

- Leads the internal and external project kickoff meetings, ensuring coordination among all stakeholders.
- Oversees project scheduling, resource allocation, and risk management activities, once the deal is closed.
- Acts as the central point of communication for project timelines and deliverables.

These individuals draw on the skills and knowledge of our software and hardware specialists, who:

- Provide expertise and support for the installation, configuration, troubleshooting and maintenance of various software and hardware systems.
- Develop and maintain documentation like user guides, manuals and policies for reference, training, and onboarding.

- Evaluate the organization's software and hardware needs, research potential solutions and make recommendations.
- Perform software upgrades, patches, data migrations during roll out of new systems.
- Diagnose problems with software applications and computer hardware reported by end users.
- Collaborate with vendors and 3rd party technicians for fixing complex software and hardware problems.
- Ensure software license compliance, audits, and asset management for inventory tracking.
- Monitor systems performance, undertake preventive maintenance, and optimize efficiency.
- Develop and conduct end-user training programs on software and hardware systems.
- Keep up to date with the latest advancements in technology to help organization stay competitive.

In essence, software and hardware specialists manage all activities pertaining to maintaining, supporting, developing, and upgrading organization's software and hardware landscape across systems.

IT Governance & Compliance. Strategic maintains full audit trails and logging for data access and cryptographic operations. Encryption practices are regularly reviewed as part of our FedRAMP/StateRAMP-aligned operational controls, and customers may request full documentation for compliance reporting and SSPs.

This standards-aligned approach ensures that all Purchasing Entities – regardless of the type or sensitivity of data – can rely on Strategics' solutions to meet or exceed applicable data protection regulations and agency security requirements.

In addition, Strategic supports the ability for customers to generate, export, and print historical, statistical, and usage reports locally, using both native cloud services and authorized third-party platforms. For customers hosted in AWS environments, Strategic enables reporting through:

- AWS CloudWatch, AWS Cost Explorer, and AWS Health Dashboard, which allow the export of usage trends, performance data, and service status reports in formats such as CSV, JSON, and PDF for local printing and offline analysis.
- CloudCheckr, which Strategic deploys for AWS customers to provide enhanced visibility into cost allocation, usage optimization, compliance posture, and reserved instance utilization. CloudCheckr supports scheduled reports, custom dashboards, and exportable documentation for audits and internal reviews.

These tools allow agencies to filter reports by resource, time frame, or account, and store outputs locally for compliance, audit, or performance tracking purposes. Similar reporting and export functionality is supported across other platforms Strategic integrates, including Azure Monitor, Google Cloud Operations Suite, and enterprise SaaS solutions. Strategic ensures these tools are configured to align with each Purchasing Entity's reporting cadence, retention policy, and governance needs.

IT Project Management (Agile, Project Management Institute (PMI)). Strategic Team applies Agile project management methodology across all client engagements, with Scrum as our standard framework. Project management deliverables include a project charter and Statement of Work (SOW), sprint plans and backlog artifacts, weekly status reports, risk registers, and formal closeout documentation. Our project managers facilitate sprint ceremonies, manage stakeholder communication, track velocity and burndown, and escalate risks proactively. For government engagements, we provide a structured documentation trail (meeting minutes, decision logs, change request records) that supports auditability and accountability throughout the project lifecycle.

Certified Project Management (PMP). Strategic's customers are supported by a well-vetted team of engineers and managers with industry-leading certifications and the experience needed to deliver solutions on time. The Director of Strategic's PMO is a certified Project Management Professional and Broadcast

Network Engineer specializing in system design, installation, configuration, remote technical support, and maintenance of broadcast equipment systems in state-of-the-art production facilities. As part of his established PMO role, he is creating a center of excellence that aligns with PMI guidelines, quality standards and company strategy. His tasks include, but are not limited to:

- Implement efficiencies that meet or exceed the financial expectations established at project initiation
- Develop and govern program and portfolio management processes, uses of dashboards, templates, keeping aligned with policies and metrics
- Monitor projects, programs and portfolio to ensure compliance with project policies and standards as well as keeping to schedules, budgets and quality expectations
- Manage project, program and portfolio deliverables and tasks
- Coach and mentor team and share knowledge and best practices
- Oversee project managers of all projects to make sure delivery of their projects is on time and within budget as well as meeting quality standards
- Reports to executive team on progress and performance of PMO
- Aid in the review of Scopes of Work and contractual agreements A/V, IT and Cloud solutions

Enterprise Architecture & Cloud Strategy. We provide application architecture and cloud strategy consulting as part of both standalone advisory engagements and integrated project delivery. Our architecture consulting covers application modernization strategy, cloud platform selection and architecture design (Azure vs. AWS), microservices vs. monolith decisions, data architecture and integration strategy, and API-first design principles. We have guided organizations through major architectural transitions, including legacy-to-cloud platform modernizations, cross-platform mobile framework migrations, and on-premise to cloud CRM transitions, delivering architectures that scale with business growth without requiring full system replacement.

2.3.4. Training Services

Our customers have access to Strategics' deep value-added technology enablement resources. Our team of certified pre-sales support will provide training as needed for specific Original Equipment Manufacturers (OEM) and CSP solutions. This is available at no cost to customers.

Strategic provides versatile training programs focused on fostering broader technology acumen for professional development. Course catalogs span both foundational and advanced skills across major solution areas like cloud, security, analytics, infrastructure, collaboration tools and emerging capabilities. These open enrollment sessions aim to cultivate practical literacies empowering teams tasked with maximizing investments in complex innovation. We tailor workshops balancing strategic roadmaps with tactical configurations so learning crystallizes into immediate execution post-instruction. By consulting overviews and deep-dives, roadmaps and lifecycles, hypotheticals and hands-on labs, our instructors activate ideas into action plans for meaningful capability uplift. Please advise if further details on general learning programs would help convey our commitment to education as transformation across people, process, and technology. As an example, Strategics' Cloud Adoption Team, led by certified experts blend interactive workshops, assessment tools and advisory engagements to guide members on ideal migration paths aligning workloads with next-generation cloud platforms. Through immersive education grounded in real-world perspectives, we empower IT leaders modernizing at the speed of community priorities balancing constituent needs with budget realities.

While Strategic is pleased to incorporate customized training engagements into SOW deployment services, specific offerings and pricing depend on distinct needs per member implementation.

Additionally, Strategic will make available all OEM based training that is targeted toward operator training to help customers troubleshoot and solve issues on their own. Much of the OEM based training is offered

at no cost to customers and in many cases, customers will be able to earn product and services certifications to help further career development. This training includes:

- Microsoft 365 & SharePoint Online
- Microsoft Project Online
- Microsoft SQL Server
- Visual Studio / Visual Studio Code
- VMware vSphere
- ESRI ArcGIS (Online, Portal, Pro)
- Azure Fundamentals & Advanced Services
- Cybersecurity Awareness & Zero Trust Principles

2.3.5. Network Support Services

- F5 BIG-IP (Load Balancing, WAF), Azure Front Door, AWS WAF, Cloudflare, etc. Due to our unique capabilities in both web/app development, web/app hosting & traditional IT we have a strong background with Azure, application load balancing, Cloudflare, and Azure Front Door. Azure is a very common application host for us with load balancing capabilities. We utilize Cloudflare for all websites in a variety of ways to enhance their security.

2.3.6. Enterprise DevOps & Cloud Services

Strategic Team applies the technologies listed in Attachment B as a standard part of application development and data platform delivery. The following describes our working proficiency across this service category.

- Cloud Architecture& Design (Azure, AWS). Strategic Team designs and implements cloud architectures on Microsoft Azure and AWS as an integral part of application delivery engagements. Our cloud architecture practice covers infrastructure design for scalability, reliability, and cost efficiency: compute tier selection (VMs, App Service, containers, serverless), managed database selection, networking and security group configuration, identity and access management, and DR planning. We have architected cloud-native SaaS platforms, coexistence data architectures across multi-system environments, and managed cloud-hosted operational platforms that scale to meet peak demand without infrastructure replacement.
- Code Deployment& CI/CD Pipelines. Strategic Team applies modern DevOps practices across all development projects. We maintain all source code in Git repositories (GitHub and GitLab), enforcing branch protection rules, pull request review requirements, and commit message standards. CI/CD pipelines are configured using GitHub Actions and GitLab CI to automate build, test, and deployment stages, ensuring that code changes are validated through automated test suites before merging and that deployment to staging and production environments is repeatable and auditable. Our pipeline configurations include static analysis (SonarQube, ESLint), unit and integration test execution, Docker image builds, vulnerability scanning (OWASP Dependency Check, npm audit), and environment-specific deployment steps. We apply semantic versioning and maintain changelogs as part of our release management discipline.
- Version Control(GitHub, GitLab). Strategic Team uses Git-based version control as a foundational engineering practice across all engagements, with GitHub and GitLab as our primary platforms. Our practices include branch protection rules, pull request reviews, commit message standards, semantic versioning, and protected tags for deployment artifacts. Repository access controls use least-privilege principles. For all engagements, source code is maintained in a client-accessible repository, with full repository history transferred at project closeout.
- IaC. Strategic Team applies IaC practices to ensure cloud infrastructure is version-controlled, repeatable, auditable, and consistently deployed across environments. Our IaC tooling includes Terraform and Azure Bicep/ARM templates for cloud resource provisioning, with IaC configurations stored in Git repositories

and subject to the same review and approval gates as application code. Environment-specific variables are managed through Azure Key Vault and AWS Secrets Manager, with no hardcoded values in templates. This ensures all infrastructure is documented, reproducible, and auditable.

- PaaS / SaaS / IaaS. Strategic Team delivers solutions across all three cloud service models as part of application development and data platform engagements. At the IaaS layer, we configure and manage Azure VMs and AWS EC2 instances for workloads requiring OS-level control. At the PaaS layer, we leverage Azure App Service, Azure Functions, AWS Lambda, and Azure Container Apps to deploy applications without managing underlying infrastructure. At the SaaS layer, we integrate and extend commercial SaaS platforms (Salesforce, HubSpot, Microsoft 365) through APIs, custom connectors, and workflow automation. Our approach selects the appropriate service model based on workload characteristics, operational requirements, and total cost of ownership.
- Containerization& Orchestration(Docker, Kubernetes). Strategic Team engineers are proficient with Docker for application containerization and Kubernetes for container orchestration. We write multi-stage Dockerfiles that produce minimal, hardened production images, configure Docker Compose for local development parity with production environments, and deploy containerized workloads to AKS and Amazon EKS. Our Kubernetes experience covers deployment manifests, services and ingress configuration, horizontal pod autoscaling, resource limits, and RBAC. We integrate container builds and image scanning into CI/CD pipelines as standard practice, ensuring that every deployment artifact is version-controlled and auditable.
- Automation &Configuration Management. Strategic Team implements automation and configuration management as standard practice in application delivery and infrastructure management. Automation capabilities include CI/CD pipeline automation (GitHub Actions, GitLab CI, Azure DevOps), infrastructure provisioning automation via IaC, database migration automation, scheduled job automation via Azure Functions and AWS Lambda, and API workflow automation connecting disparate business systems. Our automation philosophy prioritizes removing manual, error-prone processes, replacing high-volume manual workflows with reliable, auditable automated systems that scale without adding headcount.

2.4. Security & Compliance

Strategics' internally deployed security policy adheres to the baseline security controls for Cloud and Offsite Hosting implementations. Strategics' baseline security controls and security standards are aligned with NIST 800-53 security requirements such as but not limited to:

- Proper account management
- Least-privilege access control
- Remote access control
- Audit review, analysis, and reporting
- Security assessments through continuous monitoring
- Separation of duties within access control
- Session lock outs and terminations
- Security awareness and training
- Baseline configuration management
- Identification and authorization for privileged and non-privileged accounts

Strategic is a member of the Open Group Trusted Technology Forum (OTTF) and joined the OTTF in 2013. The Open Group is a standards organization which collaborates with customers and suppliers of IT products and services to identify and clarify requirements, develop standards, and openly share best practices. OTTF leads the development of a global supply chain integrity program and framework, (TOGAF – the Open Group Architecture Framework), which complies with the standards provided by ISO/IEC 20243. Strategic has an Open Trusted Technology Provider™ Standard (O-TTPS) Certification for Open Trusted Technology Provider™ V1.

Strategics' offerings exceed this requirement through continual security improvement and compliance with current and future requirements, such as NIST 800-171. Our solutions are already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately. NIST 800-171 outlines

a subset of the NIST 800-53 requirements, a guideline which has been audited under our provider's FedRAMP/StateRAMP program. The FedRAMP/StateRAMP Moderate security control baseline is more rigorous than the recommended requirements established in Chapter 3 of 800-171 and includes a considerable number of security controls beyond those required of FISMA Moderate systems that protect CUI data.

The intent to comply with all applicable laws related to data privacy and security is demonstrated through the following regulations, standards, and best practices that Strategics' offerings currently meet:

- FedRAMP
- StateRAMP
- SOC 1/AICPA AT 801
- ISO 27001
- ISO 9001
- US HIPAA
- DoD SRG security impact levels 2 and 4
- SOC 2 and 3
- FIPS 140-2
- ISO 27017
- PCI DSS
- FBI Criminal Justice Information System (CJIS)
- ISO/IEC 20243
- FERPA
- ISO 27018
- FISMA
- NIST 800-171

In addition, Strategic has carefully vetted our partners and has ensured they maintain specific certifications such as ISO 9001:2015, SCRM, Enterprise Security Policy NIST 800-145,37, 53, FedRAMP/StateRAMP if applicable.

2.4.1. Identity & Access

Strategic Team implements identity and access management at the application layer as a standard engineering practice on every engagement. For application authentication and authorization, we apply OAuth 2.0, OpenID Connect, and JWT bearer tokens with proper token lifecycle management, expiry, and rotation. RBAC is implemented within application business logic, ensuring users can only access data and functions appropriate to their role. In cloud-hosted applications, we integrate with Microsoft Entra ID (formerly Azure Active Directory) for enterprise identity, covering employee directory integration, staff and agent onboarding, password resets, and role-based permission management. We apply the principle of least-privilege to all service accounts, API keys, and database connection strings. Strategic Team is prepared to integrate with an existing Active Directory / Entra ID infrastructure for single sign-on and role synchronization. Infrastructure-level identity administration, including CAP, MFA enforcement, and Entra ID tenant management, falls outside Strategic Team' direct scope.

2.4.2. Endpoint Security

Strategic's support to endpoint security is described in our response to Section 2.4.3.

Strategic Team develops and delivers applications; we do not manage endpoint devices or deploy endpoint security tooling. For application deployments, we follow secure coding practices that minimize attack surface, including input validation, output encoding, secure session management, and no storage of sensitive data in client-side storage. Mobile applications built by Strategic Team (React Native, Flutter, iOS) are developed to platform security guidelines (Apple App Store Review, Google Play Protect requirements) and do not request unnecessary device permissions.

2.4.3. Network Security

Strategic provides both baseline and advanced security services, allowing agencies to select solutions tailored to their compliance scope, operational controls, and budget.

- Baseline Security (included, no additional cost): encryption at rest and in transit using CSP-native key management services, hardened VM templates, secure boot protocols, and isolation via Virtual Private

Clouds (VPCs) and segmentation, and logging, monitoring, and auditing using AWS CloudTrail, Azure Monitor, GCP Cloud Logging, and OCI Logging.
- Advanced Security (additional cost, typically +10%–25% of baseline): managed Detection & Response (MDR) and SOC-as-a-Service from Arctic Wolf and Trellix, Zero Trust enforcement and micro segmentation using Fortinet and Azure Network Security Groups, endpoint telemetry and cloud workload protection with CrowdStrike Falcon, compliance automation for HIPAA, CJIS, NIST 800-171, and IRS 1075 using platforms like Wiz and Fugue, and integration of hardware security modules (HSMs) and advanced key management services (KMS) policies for customer-managed encryption key ownership and rotation.

Strategic ensures all solutions are delivered on environments and platforms that maintain verifiable third-party certifications. End users retain direct access to these CSP-native controls, while Strategic layers PAC value-add services for governance and compliance.

- AWS: FedRAMP High, Department of Defense (DoD) IL4/5, System and Organization Controls (SOC) 1/2/3, ISO 27001, ISO 27017/18, PCI DSS, HIPAA, CJIS, ITAR.
- Azure (including Azure Government): FedRAMP High, DoD IL5, NIST 800-53, CJIS, IRS 1075, HITRUST.
- GCP: FedRAMP Moderate, ISO/IEC 27001/27017/27018, SOC 2 Type II, PCI DSS, HIPAA.
- OCI: SOC 1/2/3, ISO 27001/27017, FedRAMP Moderate, PCI DSS, HIPAA, GDPR, CJIS.

In addition, Strategic partners with OEMs who provide security solutions for our customers, such as:

- Arctic Wolf: SOC 2 Type II, ISO 27001 MDR platform for government.
- CrowdStrike: FedRAMP High for Falcon EDR.
- Fortinet: National Information Assurance Partnership (NIAP), Common Criteria, FIPS 140-2, ISO/IEC 27001.
- Trellix: DISA STIG-aligned, NIST 800-53 mapped.
- Ataccama: Role-based data access, masking, and lineage frameworks aligned to HIPAA/GDPR.

Strategic's security lifecycle program includes:

- Continuous vulnerability scanning (CrowdStrike Spotlight, AWS Inspector, Azure Defender, GCP Security Command Center).
- Remediation SLAs aligned to Common vulnerability scoring system (CVSS) scores and agency-specific thresholds.
- Patch management with Information Technology Infrastructure Library (ITIL) -aligned change control, notifications, and rollback plans.
- Security awareness training (KnowBe4) with quarterly phishing simulations.
- Secure software development enforced via Secure Software Development Framework (SSDF) standards across PAC integrations.

Customers retain root and account ownership, ensuring direct access to all CSP-native tools, while Strategic provides visibility and governance across platforms.

While Strategic does not publish SOC/ISO audits, we leverage certified environments from CSPs and PAC security partners, who maintain:

- SOC 2 Type II reports for MDR, SIEM, and endpoint platforms.
- ISO 27001 surveillance audits for hosted infrastructure.
- FedRAMP ATO packages via FedRAMP Marketplace.
- Third-party penetration testing and red-team assessments (artifacts available upon request).

When developing applications and software, Strategic Team enforces HTTPS with TLS 1.2+ on all application endpoints, implements HSTS headers, and configures CORS policies to restrict cross-origin access to trusted origins. For cloud-hosted applications, we configure network security groups (NSGs) and Azure Private Endpoints to restrict inbound traffic to application tiers. API gateways and application-layer rate limiting are applied to public-facing endpoints. The MDMR platform and FYX Fleet were both deployed with network-level access controls configured at the Azure infrastructure layer as part of our standard deployment architecture.

2.4.4. Monitoring & Response

Strategic provides both baseline and advanced security services, allowing agencies to select solutions tailored to their compliance scope, operational controls, and budget.

- Baseline Security (included, no additional cost): encryption at rest and in transit using CSP-native KMS, hardened VM templates, secure boot protocols, and isolation via VPCs and segmentation, and logging, monitoring, and auditing using AWS CloudTrail, Azure Monitor, GCP Cloud Logging, and OCI Logging.
- Advanced Security (additional cost, typically +10%–25% of baseline): MDR and SOC-as-a-Service from Arctic Wolf and Trellix, Zero Trust enforcement and microsegmentation using Fortinet and Azure NSGs, endpoint telemetry and cloud workload protection with CrowdStrike Falcon, compliance automation for HIPAA, CJIS, NIST 800-171, and IRS 1075 using platforms like Wiz and Fugue, and integration of HSMs and advanced KMS policies for customer-managed encryption key ownership and rotation.

Strategic ensures all solutions are delivered on environments and platforms that maintain verifiable third-party certifications. End users retain direct access to these CSP-native controls, while Strategic layers PAC value-add services for governance and compliance.

- AWS: FedRAMP High, Department of Defense (DoD) IL4/5, System and Organization Controls (SOC) 1/2/3, ISO 27001, ISO 27017/18, PCI DSS, HIPAA, CJIS, ITAR.
- Azure (including Azure Government): FedRAMP High, DoD IL5, NIST 800-53, CJIS, IRS 1075, HITRUST.
- GCP: FedRAMP Moderate, ISO/IEC 27001/27017/27018, SOC 2 Type II, PCI DSS, HIPAA.
- OCI: SOC 1/2/3, ISO 27001/27017, FedRAMP Moderate, PCI DSS, HIPAA, GDPR, CJIS.

In addition, Strategic partners with OEMS who provide security solutions for our customers, such as:

- Arctic Wolf: SOC 2 Type II, ISO 27001 MDR platform for government.
- CrowdStrike: FedRAMP High for Falcon EDR.
- Fortinet: NIAP, Common Criteria, FIPS 140-2, ISO/IEC 27001.
- Trellix: DISA STIG-aligned, NIST 800-53 mapped.
- Ataccama: Role-based data access, masking, and lineage frameworks aligned to HIPAA/GDPR.

Strategic's security lifecycle program includes:

- Continuous vulnerability scanning (CrowdStrike Spotlight, AWS Inspector, Azure Defender, GCP Security Command Center).
- Remediation SLAs aligned to CVSS scores and agency-specific thresholds.
- Patch management with ITIL -aligned change control, notifications, and rollback plans.
- Security awareness training (KnowBe4) with quarterly phishing simulations.
- Secure software development enforced via SSDF standards across PAC integrations.

Customers retain root and account ownership, ensuring direct access to all CSP-native tools, while Strategic provides visibility and governance across platforms.

While Strategic does not publish SOC/ISO audits, we leverage certified environments from CSPs and PAC security partners, who maintain:

- SOC 2 Type II reports for MDR, SIEM, and endpoint platforms.
- ISO 27001 surveillance audits for hosted infrastructure.
- FedRAMP ATO packages via FedRAMP Marketplace.
- Third-party penetration testing and red-team assessments (artifacts available upon request).

When developing apps, Strategic Team implements application-layer monitoring and alerting as a standard component of cloud deployments. This includes Azure Monitor and Application Insights for application performance monitoring, request tracing, and error alerting; AWS CloudWatch for AWS-hosted workloads; centralized structured logging (Serilog/NLog) with log aggregation; and health check endpoints on all deployed services. For the MDMR engagement, Strategic Team provides 24/7 automated monitoring of the Azure backend environment with a tiered SLA: P1 (total outage): initial response within 1 hour, resolution within one business day; P2 (partial loss of functionality): response within 4 hours; P3 (standard): response within one business day. Strategic Team is prepared to integrate application logging and telemetry with an existing SIEM platform to ensure application events flow into centralized monitoring.

2.4.5. Data Protection

Strategic follows the Federal Risk and Authorization Management Program (FedRAMP) guidelines and security guidance to protect our customers' data. Strategic's engineering team and our partner AWS provides consulting and advisory services on the creation of security controls to comply with the customers' security requirements. These services include defining the organizational scope, system scope, identify and interview system owners, regulatory factors, sensitive information storage and evaluation of AWS Cloud environments to meet or exceed security compliance requirements. Our team also helps identify high risks areas and security compliance gaps, perform system testing to validate the implementation of controls as applicable and provide code or templates to remediate non-compliant controls reported in the external audit reports. Strategic's security services span complete network coverage, endpoints, vulnerability management, monitoring, and analysis.

Continuous Monitoring. Strategic provides continuous monitoring services for any size and type of network. Our team of certified network security experts utilize state-of-the-art network monitoring tools from Cisco, Barracuda, F5, and SonicWall. Our tools provide you with accurate reporting and analytics, as well as a strategic plan to optimize your network security.

Strategic's team of network security experts provide organizations with Advanced Threat Protection. Scan email attachments, web traffic, and block malicious files from doing harm to your network. We also offer next generation firewall management; sandboxing; email gateway monitoring; web application monitoring; and end point security (anti-virus, anti-malware, anti-ransomware) design and installation.

- Implementation of the National Institute of Standards and Technology Risk Management Framework. Strategic' team of certified security experts design and architect your IT environment to meet specific security and compliance standards. Many industries mandate certain compliance standards for data security (PCI, HIPPA, CJIS, FISMA, FedRamp, etc.). Our IT team periodically assesses your environment to ensure it is always compliant and updated. We provide and install Best of Breed Internal & External Vulnerability Scanning as well as Vulnerability Reporting and Incident Management Platforms.
- Cybersecurity Posture Assessment. Our CSPs perform network penetration test to identify exploitable security vulnerabilities in networks, systems, hosts, and network devices. Security vulnerabilities allow for unauthorized access to sensitive data or even take-over systems for malicious/non-business purposes.

Strategic provides all available AWS Monitor, Manage and security services like CloudWatch, Lambda, CloudFormation, Cloud trail, WAF to monitor, manage and protect AWS Cloud/services/workloads. We also provided third-party tools and software deployments such as Splunk to add an extra layer of security and monitoring to the network cloud environment.

During Development, Strategic Team applies data protection controls at the application and database layer on every engagement. Encryption at rest is enabled for all Azure SQL and AWS RDS databases; encryption in transit is enforced via TLS 1.2+ on all data connections. Sensitive application credentials, API keys, and connection strings are stored exclusively in Azure Key Vault or AWS Secrets Manager. They are never stored in source code or configuration files. Personally identifiable information (PII) handling in application code follows data minimization principles, collecting and retaining only data necessary for the defined function. The MDMR platform adheres to ITS Enterprise Security Policies and Federal/state PII encryption standards, with WCAG 2.1 AA accessibility compliance ensuring public-facing interfaces are accessible to all users. For database backup and recovery, we configure automated backup schedules, geo-redundant backup storage, and point-in-time restore capabilities as standard for cloud-hosted databases. Strategic Team is prepared to align data handling practices with the applicable data classification policies and state or Federal data protection requirements for any given engagement.

2.4.6. Vulnerability

Strategic Team' scope: Strategic Team integrates automated vulnerability scanning into every CI/CD pipeline as a non-negotiable build gate. This includes OWASP Dependency Check and npm audit for dependency vulnerability scanning (builds containing known critical vulnerabilities are automatically blocked), and Docker image scanning prior to deployment. For cloud infrastructure, IaC templates are version-controlled and reviewed for security misconfigurations before apply. For the MDMR engagement, Strategic Team conducts quarterly vulnerability scans of the application and cloud infrastructure, applies monthly security patches to microservices and cloud infrastructure, and will facilitate an independent OWASP/NIST-aligned security audit prior to final acceptance. Application configuration is managed on a per-environment basis, with Dev, QA, and Production environments kept strictly separate, and environment promotion requiring formal approval gates.

2.4.7. Configuration Management

Strategic provides a set of tools to deploy applications including the AWS Config tool, which assesses, audits, and evaluates the configurations of all AWS resources. Config continuously monitors and records AWS resource configurations and automates the evaluation of recorded configurations against desired configurations. With the Config tool, stakeholders can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine their overall compliance against the configurations specified in internal guidelines. This simplifies compliance auditing, security analysis, change management, and operational troubleshooting.

2.4.8. Compliance Alignment

Strategic Team aligns application development and cloud architecture with the following recognized frameworks relevant to public sector engagements:

- NIST Cybersecurity Framework (CSF): Identify, Protect, Detect, Respond, and Recover functions are addressed across our SDLC, monitoring practices, incident response SLAs, and security documentation.
- NIST SP 800-53: Access control (AC) and identification/authentication control families applied in application-layer IAM design. Risk assessment (RA) practices inform architecture and threat modeling.
- NIST SP 800-37 (Risk Management Framework): RA and system authorization practices inform our architecture review and documentation for government engagements.

- NIST SP 800-218 (SSDF): Secure coding standards, vulnerability remediation processes, and software supply chain security practices applied throughout the development lifecycle.
- OWASP Top 10: All application development follows OWASP Top ten mitigation guidance. OWASP Dependency Check is integrated into CI/CD pipelines as a standard build gate.
- WCAG 2.1 AA: All public-facing applications and portals are developed to Web Content Accessibility Guidelines 2.1 Level AA, ensuring accessibility for users with disabilities, a standard requirement for government-facing systems.

2.4.9. Security Documentation

Strategic Team produces and maintains the following security-related documentation as standard deliverables for government engagements:

- SSPs: Documenting the security controls implemented within an application system, control ownership, and implementation narratives, consistent with NIST SP 800-18 format for government systems.
- Security Architecture Documentation: System diagrams illustrating authentication flows, data flows, encryption boundaries, network trust zones, and third-party integration points.
- Requirements Traceability Matrix: Linking security requirements to specific implementation decisions, test cases, and acceptance criteria.
- Vulnerability Scan Reports: Formal reports of scheduled vulnerability scan results, findings, remediation status, and residual risk acceptance, provided quarterly for maintained systems.
- Deployment Security Runbooks: Step-by-step documentation of security configuration for each deployment environment, including AC setup, secrets management, network configuration, and monitoring configuration.
- Incident Response Procedures: Defined response procedures for security incidents affecting Strategic Team-delivered applications, including notification timelines, escalation paths, and remediation protocols consistent with the client's operational requirements.

3. Engagement Model & Deliverables

We employ a hybrid project management approach combining Agile and traditional methodologies tailored to each phase of cloud implementation. Our methodology ensures structured oversight while maintaining flexibility to adapt to evolving requirements throughout the project lifecycle.

- Define the Problem: Comprehensive discovery including stakeholder interviews, current-state analysis, infrastructure assessment, requirements gathering workshops; deliverables include detailed assessment report with gap analysis, risk identification, and preliminary roadmap
- Document a Project Plan: Develop project charter defining scope, timeline, deliverables, resource allocation, success metrics; establish governance structure with steering committees, weekly status meetings, and escalation procedures.
- Architecture and Design: Architects create solution designs with security, networking, and application team input
- Implementation: Iterative Agile approach with 2-3 week sprints including planning, execution, daily standups, retrospectives; maintain detailed work breakdown structures using project management tools for real-time tracking of progress, dependencies, and risks; implement change control procedures
- Testing and Validation: Comprehensive testing including functional, performance, security, and user acceptance testing; maintain detailed test plans, test cases, and defect tracking systems; QA team works alongside implementation teams for early issue resolution
- Migration and Deployment: Detailed cutover plans with rollback procedures; deployments during maintenance windows with stakeholder notification; pre-deployment readiness reviews and post-deployment validation

- Final Installation and Handover: Knowledge transfer sessions, comprehensive documentation delivery, operational readiness verification; formal acceptance testing with stakeholders; 30-60 days hypercare support; lessons learned sessions and final project reports with metrics and recommendations

Our processes are defined in our Quality Management System, which is aligned with ISO 9001 and CMMI Level 2 standards, ensuring all processes and deliverables meet the highest quality customer service delivery criteria. Regular audits and continuous improvement initiatives are part of our QA framework. We establish mechanisms to capture and act on customer feedback, ensuring our services continually meet or exceed expectations.

4. Cost of Services (Attachment B)

Fees will depend on the requirement and length of work. Strategic maintains basic rates for infrastructure builds but other fees are dependent on project dependencies. Strategic pricing model varies depending on the type of services we provide. For Infrastructure design and install we assess hours to projects based on the Scope of Work and materials required to meet the configuration and installation of an operating system. For our enterprise solutions the model will align with the solution(cloud, software) and the resources needed based on scope and scale. Consultation requires an understanding of objectives and is often offset by a variety of partner support through grants, partner credits or initiatives. Strategic has maintained consulting fees at nearly zero cost to our clients but when there are fees, they are specific to the project and cannot be defined at this time.

Basic rates:

Project Management: $164

Design engineering (Infrastructure) $160

Technician (Infrastructure) $108

5. Company Information

5.1. Company and Years in Business.

Strategic Communications, LLC (Strategic) was founded in 1994 and offers 32 years of successful experience supporting State, Local, and Federal customers.

5.2. Business Partnerships

Strategic's is well-equipped to provide IaaS, PaaS, and SaaS from the major public cloud providers, specifically AWS, Microsoft Azure, Google Cloud Platform (GCP), and OCI. Our cloud offerings include but are not limited to:

- AWS: With its broad range of compute, storage, networking, and security services, AWS offers unmatched scalability and flexibility for a wide array of enterprise needs, including advanced analytics, machine learning, and application modernization.
- Microsoft Azure: Azure's strengths in hybrid cloud, enterprise integrations, and support for Microsoft-centric environments make it an ideal platform for organizations looking to leverage both cloud and on-premises resources with strong compliance and security controls.
- GCP: GCP provides state-of-the-art solutions for data analytics, machine learning, and AI. Its innovative capabilities enable the State to harness the power of data-driven decision-making and innovative, scalable infrastructure solutions.

- OCI: Known for its robust database management and enterprise application services, OCI is tailored for mission-critical workloads and high-performance computing environments, providing a strong platform for applications requiring stringent security and performance standards.

Additionally, Strategic's offering goes beyond these four providers to include solutions from over 3,505 technology partners, ensuring Kentucky has access to the most appropriate and cost-effective cloud resources for each unique workload. Strategics' vision is to provide the knowledge, resources, and innovative solutions, delivered through an alliance of IT partners capable of resolving critical challenges indirectly or directly impacting citizens. To realize this vision, Strategic created the PAC in 2021. Our PAC currently consists of CSPs, Distributors, OEM, and ISV. Strategic is continuously expanding our PAC as we onboard more trusted partners who share our passion for public sector IT excellence.

Strategic has teamed with two companies that enhance our capabilities to deliver exceptional services on this contract:

- Founded in 2004, Louisville Geek has grown from a local computer repair shop into a leading managed IT services provider supporting businesses across Kentucky and the United States. The company delivers managed services, cybersecurity, cloud solutions, co-managed IT support, and process automation through a team of engineers, project managers, and developers committed to clear communication and reliable results. The company is a privately owned, EOS run and SOC 2 compliant organization that focuses on predictable outcomes, strong partnerships, and long-term value for every client.
- FocustApps is a full-service custom software development and technology consulting firm headquartered in Louisville, Kentucky. The company specializes in designing, building, and delivering scalable, high-performance software solutions across web, mobile, cloud, and enterprise platforms. FocustApps brings deep expertise across the full SDLC, from requirements gathering and architecture design through implementation, integration, QA, deployment, and ongoing support. In addition, FocustApps has a demonstrated track record of partnering with organizations across logistics, manufacturing, healthcare, field services, enterprise operations, and the public sector to solve complex technology challenges. We have direct experience working with state government agencies, most notably as the awarded vendor for the MDMR Fishing License Platform and Mobile Application, giving us firsthand familiarity with the operational, compliance, and procurement considerations that define public sector technology engagements, including data governance requirements, auditability, and the need for transparent, deliverable-based project structures.

5.3. References

Strategic Communications delivers comprehensive consulting services across cloud modernization, cybersecurity, DevSecOps, data engineering, and mission-critical application delivery. Our approach is rooted in proven federal past performance and aligned with compliance frameworks such as FedRAMP, FISMA Moderate/High, and DoD IL requirements. The following outlines our capabilities across key service areas, supported by relevant past performance.

Strategic Communications brings deep experience supporting federal and state agencies in highly regulated environments requiring secure, scalable, and resilient solutions.

- United States Air Force Kessel Run. Delivered cloud-native DevSecOps enablement and platform engineering support for mission-critical applications. Enabled rapid software delivery through CI/CD pipelines, containerization (Kubernetes), and infrastructure-as-code (IaC) within secure DoD environments.
- Defense Health Agency. Supported healthcare data modernization initiatives, including secure data migration, interoperability, and analytics platforms compliant with HIPAA, FISMA High, and DoD IL5 standards. Focused on ensuring availability and integrity of mission-critical health systems.

- Mississippi Cloud Service Provider and Value-Added Reseller (CSPV) Program Provides cloud consulting, procurement, and managed services across state agencies. Delivered cloud migration, cost optimization, and governance using AWS-native services with transparent billing, FinOps practices, and continuous optimization reporting.

Our consulting methodology is structured, repeatable, and aligned to federal best practices (Exhibit 3):

Task	Practices
Discover & Assess	• Conduct cloud readiness assessments, application dependency mapping, and security posture evaluations • Leverage automated tools and workshops to define current-state vs. target-state architectures
Design & Architect	• Develop secure, scalable architectures aligned to AWS Well-Architected Framework and Zero Trust principles • Define landing zones, governance models, and compliance guardrails (e.g., FedRAMP, NIST 800-53)
Build & Migrate	• Execute migrations using AWS Migration Acceleration Program (MAP) methodologies • Implement DevSecOps pipelines, container platforms, and serverless architectures
Operate & Optimize	• Provide ongoing managed services, monitoring, and cost optimization (FinOps) • Deliver continuous improvement through monthly reporting, KPIs, and automation enhancements

Exhibit 3, Strategic Follows Compliant Best Practices.

Security & Resilience

Security is embedded at every layer of our consulting services, leveraging a "secure-by-design" philosophy.

Core Capabilities:

- Zero Trust Architecture implementation (identity-first, least privilege access)
- Continuous monitoring aligned with NIST SP 800-137 and FedRAMP Continuous Monitoring
- Data protection using encryption (FIPS 140-2 validated), tokenization, and secure key management
- Integration of SIEM/SOAR platforms (e.g., Splunk, AWS Security Hub, GuardDuty)

Resilience Engineering:

- Multi-AZ and multi-region architectures for high availability
- Automated failover and self-healing infrastructure
- Chaos engineering and resilience testing

Past Performance Alignment:

- Kessel Run: Secure CI/CD pipelines within hardened DoD environments
- DHA: Protection of sensitive healthcare data with high availability requirements
- Mississippi CSPV: Statewide governance, security baselines, and compliance enforcement

Business Continuity / Disaster Recovery (BC/DR)

Strategic Communications designs and implements robust BC/DR strategies to ensure mission continuity.

Capabilities Include:

- Business Impact Analysis (BIA) and Recovery Time Objective (RTO) / Recovery Point Objective (RPO) definition
- Automated backup and recovery using AWS-native services (e.g., AWS Backup, S3 lifecycle policies)
- Cross-region replication and pilot-light / warm standby / active-active DR architectures
- Regular DR testing, validation, and runbook development

Approach:

- Align BC/DR strategies to agency mission priorities and compliance requirements
- Implement Infrastructure-as-Code for rapid environment reconstitution
- Provide continuous monitoring and alerting for failover readiness

Strategic Communications combines proven federal experience, a structured delivery methodology, and a security-first mindset to deliver consulting services that are scalable, compliant, and resilient. Our past performance with Air Force Kessel Run, the Defense Health Agency, and the Mississippi CSPV program demonstrates our ability to successfully support complex, mission-critical environments while ensuring operational continuity and cost efficiency.

6. Additional Information & Contract Terms

Strategic does not have a standard contract.

Strategic agrees that all materials developed, data collected, or reports prepared under the project agreement become the property of LFUCG. LFUCG reserves non-exclusive rights to copy, publish, disseminate, and use materials developed under the agreement, in print or electronically.

Strategic acknowledges public records obligations, auditability, and operational resiliency requirements typical of government environments.

7. Past Performance

Exhibit 4 summarizes Strategic Team' key project engagements relevant to both Attachment A and Attachment B. Projects are ordered by regulatory complexity and public sector relevance. Full case studies are available upon request.

Client / Project	Technologies	Relevance & Capability Demonstrated
Maryland State Department of Education (MSDE)	A wide variety of AWS Cloud-hosted solutions including, Application Hosting, Database Services, DB Instances, Non-Relational Database (DynamoDB), Storage, Data Transfer, Maintenance and Support, Consulting Services, and other cloud services. This is a cooperative contract that allows State of Maryland agencies access to technical cloud environments. The three cloud categories awarded are IaaS, SaaS, and PaaS.	MSDE) engaged Strategic Communications, in collaboration with AWS Professional Services, to support a large-scale data center exit and cloud enablement initiative. The customer needed to migrate more than 400 servers from an on-premises environment by the end of 2026, where they were incurring approximately $1.17M annually in infrastructure costs. Rather than outsourcing the migration execution, the project focused on equipping MSDE and Maryland Department of IT's (DoIT) internal teams with the skills, training, and documentation required to design and operate secure, scalable cloud architectures in AWS, aligned to industry best practices. Through structured training sessions, hands-on guidance, and reusable architectural documentation, MSDE's staff built the skills to complete the remaining migration activities independently. As a result of the move to AWS, DoIT estimates up to 35% annual cost savings compared to the legacy environment, with a projected break-even point of approximately nine months after professional services costs. This engagement demonstrates a proven approach to accelerating cloud adoption while reducing long-term costs and building sustainable internal expertise.

Client / Project	Technologies	Relevance & Capability Demonstrated
National Science Foundation	AWS Cloud provider	Strategics' engineers designed a multi-cloud approach to meet NSFs' stringent requirements. Strategic designed an on-demand, self-service IaaS for NSF that delivered a dependable, responsive, and cost-effective cloud-based service to help, improve manageability, increase flexibility, reduce complexity of existing data center hosting hardware, software, and operations and to provide an expanded service to the applications owners and end users. Strategic also provided a comprehensive list of our offered electronic and IT products and services that fully comply with Section 508 clauses and agency security requirements such as Safeguarding Information, Controlled Unclassified Information, Homeland Security Directives Privacy Act, and much more were incorporated into the award.
State of Maryland	AWS Cloud provider	Our scope of services includes account and identity service, account maintenance, network, application, software, managed services, cloud migration services, a customized billing platform and application management. In addition, we are providing technical training on multi-cloud environments for SOM engineers in the event they decide to deploy a multi-cloud approach to their existing environment. Strategic offers SOM over two hundred fully featured cloud services including IaaS, PaaS, and SaaS, and compute. Strategic also provides a variety of network services deployed within their cloud environment, such as Elastic Load Balancing, CloudFront, Route 53, Direct Connect, VPC, VPN, Transit Gateway, and Cloud Map. These services enabled SOM to effectively maintain network connectivity and security for their applications on-premises and on the cloud. Strategic also provides numerous tools to enable SOM to deploy Enterprise-wide Innovation Services_applications. For example: • The Config tool assesses, audits, and evaluates the configurations of all AWS resources against desired configurations. SOM stakeholders can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine their overall compliance against the configurations specified in internal guidelines to simplify compliance auditing, security analysis, change management, and troubleshooting. • The AWS Management Console helps SOM manage all available AWS resources in a single destination, from Amazon EC2 instances to Amazon DynamoDB tables. The console also enables SOM to manage all aspects of their data accounts, including accessing monthly spending by service, managing security credentials, or even setting up new IAM users. This console supports all AWS Cloud Regions and allows Strategic and SOM engineers to provision resources across multiple regions. • A secure dedicated environment for software developers allows SOM to deploy proof of concept ideas in a test environment. • AWS Connect delivers a robust cloud contact center. AWS Connect supports omnichannel interactions across voice and chat, enabling seamless communication and efficient issue resolution through skills-based routing and real-time analytics. It integrates with other AWS services and external applications, providing a comprehensive and scalable platform.
Mississippi Dept. of Marine Resources(MDMR - Awarded)Fishing	.NET 8 microservices, React Native (offline-first mobile), Azure SQL, Azure Cloud, CI/CD/IaC,	Direct state government engagement. Strategic Team was awarded the contract to design and deliver Mississippi MDMR's next-generation Fishing License Platform and Mobile Application. Platform serves the general public, administrative staff, and Marine Patrol enforcement officers (offline-first field

Client / Project	Technologies	Relevance & Capability Demonstrated
License Platform & Mobile App	REST APIs, Tyler Technologies payment integration, ESRI ArcGIS geospatial integration, NOAA API, ETL/SQL Server migration, WCAG 2.1 AA	tools in zero-connectivity coastal environments). Key scope: .NET 8 microservices backend with automated rules engine (70+ license types); React Native offline-first mobile app; Tyler Technologies POS/payment integration; ESRI ArcGIS geofenced mapping; multi-language support (English, Spanish, Vietnamese); ETL migration from legacy SQL Server; OWASP/NIST security audit; WCAG 2.1 AA accessibility; 3-year post-warranty SLA (P1 response within 1 hour). Delivered under a Sequential Phase-Gate methodology with formal state agency sign-offs. Strategic Team' most direct public sector reference.
FYX Fleet(MRP Platform)	Azure Cloud, Power BI, REST APIs, SaaS platform, payment APIs, automated workflows, SQL database	DOT/transportation sector, federally regulated. Modern Azure SaaS platform replacing legacy AS400 MRP system. Customer/vendor portal, automated workflows, Power BI analytics, API-powered payment system. Service events scaled from 40K to 70K in 3 months; $17.7M revenue increase. Demonstrates high-volume, mission-critical operational platform development directly relevant to LFUCG operational systems.
Miner Corporation(SafeCheck)	Mobile/web app, Azure cloud, database design, asset management, Occupational Safety and Health Administration (OSHA) compliance reporting, predictive maintenance	Regulated warehouse and logistics sector, OSHA compliance environment. Facility management application centralizing asset data, automating OSHA compliance documentation, and enabling predictive maintenance. Directly parallels LFUCG public facility asset management, safety compliance, and operational monitoring needs.
Concentric(RAAMS)	Web app, real-time IoT data, REST APIs, GPS/location, predictive analytics, database design, mobile	Regulated critical power/industrial sector. Custom web application for real-time IoT forklift battery management across multi-facility operations. REST APIs, real-time data ingestion, historical database design, GPS location tracking, and predictive maintenance, relevant to LFUCG infrastructure monitoring and field operations use cases.
Enterprise MDM(Facilities & Material-Handling)	Azure MDM architecture, enterprise schema mapping, ETL/deduplication, ML-driven categorization, RBAC, event-driven data refresh, Power BI, eight platforms, 70,000+ SKUs	Regulated facilities management and distribution environment. Azure coexistence of MDM architecture unifying eight systems, 70,000+ SKUs. 25% reduction in reporting time, ~130 hours/week saved, 5x data refresh cycles, 1,360 ML automation hours saved, 10% customer retention improvement, 100% self-service BI adoption, with no core system replacement.
OCR Invoice Automation(Facilities Services)	OCR document ingestion, AI-assisted exception handling, workflow automation, system integration, iterative Time and Materials (T&M) delivery	Regulated facilities services sector, high-volume financial processing. OCR-based invoice ingestion, AI-assisted exception handling, workflow automation, and system integration eliminating ~50% of manual invoice processing (hundreds of thousands annually). 40–50% no-touch rate, payment terms restored to net 30, zero added headcount.
Franklin Electric(Flutter Migration)	.NET, Flutter, Dart, iOS, Android, CI/CD, App Store deployment	Manufacturing sector. Full mobile app rebuild from Cordova to Flutter. Cross-platform iOS/Android, formal use case methodology, rigorous QA, App Store deployment. Demonstrates structured SDLC and dedicated QA engineering.

Client / Project	Technologies	Relevance & Capability Demonstrated
Headwater Companies(Hub App)	iOS, Swift, Azure Active Directory, offline-first architecture, CRM module, SQLite	Industrial sector, remote field operations. Offline-first iOS application with Azure AD integration, location directory, custom CRM module, and field status reporting, relevant to LFUCG field services and remote workforce scenarios.
OnPoint Group(Salesforce Migration)	Data migration, ETL, Salesforce, HubSpot, Marketing Cloud, CRM customization, change management	Enterprise facility maintenance. Full CRM data migration from HubSpot to Salesforce: ETL, data cleansing, transformation, Salesforce customization, Marketing Cloud integration, user training, and post-migration support.
FocustDNA(BI Platform)	Business intelligence, AI/ML integration, managed data hosting, Power BI, proactive data monitoring	Proprietary managed BI platform. AI-driven analytics, proactive data monitoring, managed hosting, Power BI integration. 124 reports across six business units, 580 users, demonstrating managed data platform delivery relevant to LFUCG analytics needs.
Total Fleet Solutions(HubSpot Integration)	WordPress, PHP, Gravity Forms, HubSpot REST API, workflow automation, UTM/campaign tracking	Fleet management sector. Gravity Forms to HubSpot CRM integration via custom API. Full field mapping, workflow automation, UTM tracking, automated contact creation, error logging with failover.
PaperCone(FedEx API Integration)	REST API integration, Visual Basic desktop, automated workflows, label generation, real-time tracking	Packaging/logistics sector. Custom FedEx API integration within existing Visual Basic desktop application, enabling automated shipment creation, label generation, real-time tracking, zero workflow disruption.
PowerHive ROI Calculator(Fleet Maintenance)	Web-based application (fixed-bid), standardized business logic, HubSpot CRM API integration, automated lead capture, ASP.NET Core / JavaScript frontend	Fleet maintenance sector. Fixed-bid web-based ROI calculator with HubSpot CRM integration and automated lead capture. Nearly $1B in potential customer savings illustrated; consistent ROI delivery across distributed sales team.

Exhibit 4, Relevant Past Performance

8. Additional Contract Documentation

Strategic's contract documentation is attached as follows:

- Attachment A, Technical Services Affidavit
- Attachment B, EEO Agreement
- Attachment C, Workforce Analysis
- Attachment D, Notice of Small Business (SB) Requirement
- Attachment E, LFUCG MWDBE Participation Form and WBE Certification
- Attachment F, General Provisions
- Attachment G, Insurance Coverage

Attachment A, Technical Services Affidavit

AFFIDAVIT

Comes the Affiant, Kathy Mills, and after being first duly sworn, states under penalty of perjury as follows:

1. His/her name is Kathy Mills and he/she is the individual submitting the proposal or is the authorized representative of Strategic Communications, LLC, the entity submitting the proposal (hereinafter referred to as "Proposer").

2. Proposer will pay all taxes and fees, which are owed to the Lexington-Fayette Urban County Government at the time the proposal is submitted, prior to award of the contract and will maintain a "current" status in regard to those taxes and fees during the life of the contract.

3. Proposer will obtain a Lexington-Fayette Urban County Government business license, if applicable, prior to award of the contract.

4. Proposer has authorized the Division of Procurement to verify the above-mentioned information with the Division of Revenue and to disclose to the Urban County Council that taxes and/or fees are delinquent or that a business license has not been obtained.

5. Proposer has not knowingly violated any provision of the campaign finance laws of the Commonwealth of Kentucky within the past five (5) years and the award of a contract to the Proposer will not violate any provision of the campaign finance laws of the Commonwealth.

6. Proposer has not knowingly violated any provision of Chapter 25 of the Lexington-Fayette Urban County Government Code of Ordinances, known as "Ethics Act."

7. Proposer acknowledges that "knowingly" for purposes of this Affidavit means, with respect to conduct or to circumstances described by a statute or ordinance defining an offense, that a person is aware or should have been aware that his conduct is of that nature or that the circumstance exists.

Continued on next page

8. Bidder will comply with all registration requirements as a contractor where required by Section 5-85 of the Code of Ordinances of the Lexington-Fayette Urban County Government. Bidder will utilize as subcontractors on the contract only contractors who are registered as required by Section 5-85 of the Code of Ordinances. Bidder will maintain a "current" status with regard to all contractor registration requirements during the life of the contract and will ensure that all subcontractors maintain a "current" status with regard to all contractor registration requirements during the life of the contract. Bidder has authorized the Division of Procurement to verify the registration of Bidder and Bidder's subcontractors with the Division of Building Inspection.

Further, Affiant sayeth naught.

Kathy Mills

STATE OF Kentucky

COUNTY OF Jefferson

The foregoing instrument was subscribed, sworn to and acknowledged before me by Kathy Mills on this the 15th day of April, 2026.

My Commission expires: 06/13/2029

Paige Rea
NOTARY PUBLIC, STATE AT LARGE

PAIGE ALEXIS REA
Notary Public
Commonwealth of Kentucky
Commission Number KYNP28569
My Commission Expires Jun 13, 2029

Attachment B, EEO Agreement

EQUAL OPPORTUNITY AGREEMENT

Standard Title VI Assurance

The Lexington Fayette-Urban County Government, (hereinafter referred to as the "Recipient") hereby agrees that as a condition to receiving any Federal financial assistance from the U.S. Department of Transportation, it will comply with Title VI of the Civil Rights Act of 1964, 78Stat.252, 42 U.S.C. 2000d-4 (hereinafter referred to as the "Act"), and all requirements imposed by or pursuant to Title 49, Code of Federal Regulations, U.S. Department of Transportation, Subtitle A, Office of the Secretary, (49 CFR, Part 21) Nondiscrimination in Federally Assisted Program of the Department of Transportation – Effectuation of Title VI of the Civil Rights Act of 1964 (hereinafter referred to as the "Regulations") and other pertinent directives, no person in the United States shall, on the grounds of race, color, national origin, sex, age (over 40), religion, sexual orientation, gender identity, veteran status, or disability be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity for which the Recipient receives Federal financial assistance from the U.S. Department of Transportation, including the Federal Highway Administration, and hereby gives assurance that will promptly take any necessary measures to effectuate this agreement. This assurance is required by subsection 21.7(a) (1) of the Regulations.

The Law

- Title VII of the Civil Rights Act of 1964 (amended 1972) states that it is unlawful for an employer to discriminate in employment because of race, color, religion, sex, age (40-70 years) or national origin.
- Executive Order No. 11246 on Nondiscrimination under Federal contract prohibits employment discrimination by contractor and sub-contractor doing business with the Federal Government or recipients of Federal funds. This order was later amended by Executive Order No. 11375 to prohibit discrimination on the basis of sex.
- Section 503 of the Rehabilitation Act of 1973 states:

  The Contractor will not discriminate against any employee or applicant for employment because of physical or mental handicap.

- Section 2012 of the Vietnam Era Veterans Readjustment Act of 1973 requires Affirmative Action on behalf of disabled veterans and veterans of the Vietnam Era by contractors having Federal contracts.
- Section 206(A) of Executive Order 12086, Consolidation of Contract Compliance Functions for Equal Employment Opportunity, states:

  The Secretary of Labor may investigate the employment practices of any Government contractor or sub-contractor to determine whether or not the contractual provisions specified in Section 202 of this order have been violated.

****

The Lexington-Fayette Urban County Government practices Equal Opportunity in recruiting, hiring and promoting. It is the Government's intent to affirmatively provide employment opportunities for those individuals who have previously not been allowed to enter into the mainstream of society. Because of its importance to the local Government, this policy carries the full endorsement of the Mayor, Commissioners, Directors and all supervisory personnel. In following this commitment to Equal Employment Opportunity and because the Government is the benefactor of the Federal funds, it is both against the Urban County Government policy and illegal for the Government to let contracts to companies which knowingly or unknowingly practice discrimination

in their employment practices. Violation of the above mentioned ordinances may cause a contract to be canceled and the contractors may be declared ineligible for future consideration.

Please sign this statement in the appropriate space acknowledging that you have read and understand the provisions contained herein. Return this document as part of your application packet.

Bidders

I/We agree to comply with the Civil Rights Laws listed above that govern employment rights of minorities, women, Vietnam veterans, handicapped and aged persons.

Paige Rew
Signature

Strategic Communications, LLC
Name of Business

Attachment C, Workforce Analysis

WORKFORCE ANALYSIS FORM

Name of Organization: Strategic Communications LLC

Categories	Total	White (Not Hispanic or Latino)		Hispanic or Latino		Black or African-American (Not Hispanic or Latino		Native Hawaiian and Other Pacific Islander (Not Hispanic or Latino		Asian (Not Hispanic or Latino		American Indian or Alaskan Native (not Hispanic or Latino		Two or more races (Not Hispanic or Latino		Total	
		M	F	M	F	M	F	M	F	M	F	M	F	M	F	M	F
Administrators																	
Professionals	22	11	2	3		3	1			1				1		19	3
Superintendents																	
Supervisors	15	7	5								1		1	1		8	7
Foremen																	
Technicians	8	6		2												8	
Protective Service																	
Para-Professionals																	
Office/Clerical	51	23	16	1	1	3	4				1				2	27	24
Skilled Craft																	
Service/Maintenance																	
Total:	96	47	23	6	1	6	5			1	3		1	2	4	62	34

Prepared by: Paige Reh **Date:** 04 / 13 / 2026

(Name and Title)

Revised 2015-Dec-15

Attachment D, Notice of Small Business (SB) Requirement

DIRECTOR, DIVISION OF PROCUREMENT
LEXINGTON-FAYETTE URBAN COUNTY GOVERNMENT
200 EAST MAIN STREET
LEXINGTON, KENTUCKY 40507

NOTICE OF REQUIREMENT FOR AFFIRMATIVE ACTION TO ENSURE EQUAL EMPLOYMENT OPPORTUNITIES AND DBE CONTRACT PARTICIPATION

The Lexington-Fayette Urban County Government has a Certified Minority and Women Business Enterprise seventeen percent (17%) minimum goal including minimum subgoals of five percent (5%) for Minority Business Enterprises (MBE) and a subgoal of twelve percent (12%) for Women Business Enterprises (WBE); a three (3%) minimum goal for Certified Veteran-Owned Small Businesses and/or Certified Service- Disabled Veteran Owned Businesses; and a goal of utilizing Disadvantaged Business Enterprises (DBE), where applicable, for government contracts.

For assistance in locating certified DBEs, MBEs, WBEs, VOSBs and/or VOSBs, contact Sherita Miller at 859/258-3320 or by writing the address listed below:

Sherita Miller, MPA, CPSD
Minority Business Enterprise Liaison
Division of Procurement
Lexington-Fayette Urban County Government
200 East Main Street
Lexington, Kentucky 40507
smiller@lexingtonky.gov
859-258-3323

Firm Submitting Proposal: Strategic Communications, LLC

Complete Address: 310 EVERGREEN ROAD, LOUISVILLE, KY, 40243
Street City Zip

Contact Name: Paige Reh Title: Director of HR & Administration

502-493-7234

Telephone Number: 502-813-8048 Fax Number: _____

Email address: preh@yourstrategic.com

Attachment E, LFUCG MWDBE Participation Form and WBE Certification

WBENC
WOMEN'S BUSINESS ENTERPRISE NATIONAL COUNCIL
JOIN FORCES. SUCCEED TOGETHER.

HEREBY GRANTS
WOMAN OWNED SMALL BUSINESS (WOSB) CERTIFICATION TO

Strategic Communications, LLC

The identified small business is an eligible WOSB for the WOSB Program, as set forth in 13 C.F.R. part 127 and has been certified as such by an SBA approved Third Party Certifier pursuant to the Third Party Agreement, dated June 30, 2011, and available at www.sba.gov/wosb.

The WOSB Certification expires on the date herein unless there is a change to the SBA's regulation that makes the WOSB ineligible or there is a change in the WOSB that makes the WOSB ineligible. If either occurs, this WOSB Certification is immediately invalid. The WOSB must not misrepresent its certification status to any other party, including any local or State government or contracting official or the Federal government or any of its contracting officials.

Majority Female Owner: Stella Kathy Mills
NAICS: 541519, 334111, 334112, 334118, 334210, 334220, 334290, 334310, 334417 UNSPSC: 41106312, 43000000, 43200000, 43210000, 43211500, 43211501, 43211502, 43211503, 43211506, 43211507, 43211508, 56112001, 56112005, 80101507, 80111716, 80111800, 80111801, 81141902, 81160000, 86141702
Certification Number: WOSB180419
Renewal Date: December 31, 2024
WOSB Regulation Expiration Date: 12/31/2026

WBECORV
WOMEN'S BUSINESS ENTERPRISE COUNCIL OHIO RIVER VALLEY

Lynnise Smith, Women's Business Enterprise Council Ohio River Valley Executive Director

Pamela Prince-Easton, WBENC President & CEO

LaKesha White, Vice President, Certification

LEXINGTON

MINORITY BUSINESS ENTERPRISE PROGRAM

Sherita Miller, MPA, CPSD
Minority Business Enterprise Liaison
Division of Procurement
Lexington-Fayette Urban County Government
200 East Main Street
Lexington, KY 40507
smiller@lexingtonky.gov
859-258-3323

OUR MISSION: The mission of the Minority Business Enterprise Program (MBEP) is to facilitate the full participation of minority and women owned businesses in the procurement process and to promote economic inclusion as a business imperative essential to the long- term economic viability of Lexington-Fayette Urban County Government.

To that end the urban county council adopted and implemented Resolution 272-2024 – a Certified Minority and Women Business Enterprise seventeen percent (17%) minimum goal including minimum subgoals of five percent (5%) for Minority Business Enterprises (MBE) and a subgoal of twelve percent (12%) for Women Business Enterprises (WBE); a three (3%) minimum goal for Certified Veteran-Owned Small Businesses and/or Certified Service- Disabled Veteran Owned Businesses; and a goal of utilizing Disadvantaged Business Enterprises (DBE), where applicable, for government contracts.

The resolution states the following definitions shall be used for the purposes of reaching these goals:

Certified Disadvantaged Business Enterprise (DBE) *– a business in which at least fifty-one percent (51%) is owned, managed and controlled by a person(s) who is socially and economically disadvantaged as define by 49 CFR subpart 26.*

Certified Minority Business Enterprise (MBE) *– a business in which at least fifty-one percent (51%) is owned, managed and controlled by an ethnic minority (i.e. Black American, Asian American, Hispanic American, Native American)*

Certified Women Business Enterprise (WBE) *– a business in which at least fifty-one percent (51%) is owned, managed and controlled by a woman.*

Certified Veteran-Owned Small Business (VOSB) *– a business in which at least fifty-one percent (51%) is owned, managed and controlled by a veteran who served on active duty with the U.S. Army, Air Force, Navy, Marines or Coast Guard.*

Certified Service -Disabled Veteran Owned Small Business (SDVOSB) *– a business in which at least fifty-one percent (51%) is owned, managed and controlled by a disabled veteran who served on active duty with the U.S. Army, Air Force, Navy, Marines or Coast Guard.*

The term "Certified" shall mean the business is appropriately certified, licensed, verified, or validated by an organization or entity recognized by the Division of Procurement as having the appropriate credentials to make a determination as to the status of the business.
The following certifications are recognized and accepted by the MBEP:

Kentucky Transportation Cabinet (KYTC), Disadvantaged Business Enterprise (DBE)
Kentucky Minority and Women Business Enterprise (MWBE)
Women's Business Enterprise National Council (WBENC)
National Women Business Owners Corporation (NWBOC)
National Minority Supplier Development Council (NMSDC)
Tri-State Minority Supplier Development Council (TSMSDC)
U.S. Small Business Administration Veteran Small Business Certification (VetCert)
Kentucky Service- Disabled Veteran Owned Small Business (SDVOSB)

To comply with Resolution 272-2024, prime contractors, minority and women business enterprises, veteran owned small businesses, and service-disabled veteran owned small businesses must complete monthly contract compliance audits in the Diverse Business Management Compliance system, https://lexingtonky.diversitycompliance.com/

A list of organizations that certify and/or maintain lists of certified businesses (i.e. DBE, MBE, WBE, VOSB and/or SDVOSB) is available upon request by emailing, Sherita Miller, smiller@lexingtonky.gov.

LEXINGTON

LFUCG MWDBE PARTICIPATION FORM
Bid/RFP/Quote Reference # 12-2026 Information Technology Consulting & Technical Services

The MWDBE and/or veteran subcontractors listed have agreed to participate on this Bid/RFP/Quote. If any substitution is made or the total value of the work is changed prior to or after the job is in progress, it is understood that those substitutions must be submitted to the Division of Procurement for approval immediately. **Failure to submit a completed form may cause rejection of the bid.**

MWBE Company, Name, Address, Phone, Email	DBE/MBE WBE/VOSB/SDVOSB	Work to be Performed	Total Dollar Value of the Work	% Value of Total Contract
1. Strategic Communications, LLC 310 Evergreen Road Louisville, KY, 40243 502-493-7234 info@yourstrategic.com	MBE/WBE	IT Services Prime	TBD	17% or more
2. Constructive Curiosity Walton, KY contactus@ 859-208-4343 constructivecuriosity.com	VOSB	PMaaS & SaaS IT Services Sub	TBD	3%
3.				
4.				

The undersigned company representative submits the above list of MDWBE and veteran firms to be used in accomplishing the work contained in this Bid/RFP/Quote. Any misrepresentation may result in the termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

Strategic Communications, LLC
Company

Paige Reh
Company Representative

Date **Title**

LEXINGTON

LFUCG MWDBE SUBSTITUTION FORM
Bid/RFP/Quote Reference #_____

The substituted MWDBE and/or veteran subcontractors listed below have agreed to participate on this Bid/RFP/Quote. These substitutions were made prior to or after the job was in progress. These substitutions were made for reasons stated below and are now being submitted to the Division of Procurement for approval. By the authorized signature of a representative of our company, we understand that this information will be entered into our file for this project. **Note: Form required if a subcontractor is being substituted on a contract.**

SUBSTITUTED DBE/MBE/WBE/VOSB Company Name, Address, Phone, Email	DBE/MBE/WBE/VOSB/SDVOSB Formally Contracted/ Name, Address, Phone, Email	Work to Be Performed	Reason for the Substitution	Total Dollar Value of the Work	% Value of Total Contract
1.					
2.					
3.					
4.					

The undersigned acknowledges that any misrepresentation may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

_____ _____
Company **Company Representative**

_____ _____
Date **Title**

LEXINGTON

DOCUMENTATION REQUIRED FOR GOOD FAITH EFFORTS AND OUTREACH PLANS

As affirmed in Resolution Number 272-2024, the Urban County Council has adopted an annual aspirational goal of utilizing at least seventeen percent (17%) of public funds spend from certain discretionary agreements with certified Minority Business Enterprises (MBEs) and certified Woman Business Enterprises (WBEs); utilizing at least three percent (3%) of public funds from certain discretionary agreements with Certified Veteran-Owned Small Business and Certified Service-Disabled Veteran-Owned Small Businesses (VOSBs); and utilizing Disadvantaged Business Enterprises (DBEs) where applicable. Bidders should make every effort to achieve these goals.

Therefore, as an element of the responsiveness of the bid, all Bidders are required to submit documentation of their good faith and outreach efforts to ensure all businesses, including small and disadvantaged businesses such as minority-, woman-, and veteran-owned businesses, have an equal opportunity to compete for and participate in the performance of any subcontracts resulting from this procurement. Examples of good faith and outreach efforts that satisfy this requirement to encourage the participation of, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs include:

1. Advertised opportunities to participate in the contract in at least two (2) publications of general circulation media; trade and professional association publications; small and minority business or trade publications; and publications or trades targeting minority, women, and disadvantaged businesses not less than fifteen (15) days prior to the deadline for submission of bids to allow, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs to participate.

2. Attended LFUCG Procurement Economic Inclusion Outreach event(s) within the past year to meet new small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs to partner with on LFUCG contracts and procurements.

3. Attended pre-bid/pre-proposal meetings that were scheduled by LFUCG to inform small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs of subcontracting opportunities.

4. Sponsored Economic Inclusion event to provide networking opportunities for prime contractors and small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs.

5. Requested a list of certified small, DBE, MBE, WBE, VOSB and/or SDVOSB subcontractors or suppliers from LFUCG and showed evidence of contacting the companies on the list(s).

6. Contacted organizations that work with small, DBE, MBE, WBE, and VOSB companies for assistance in finding certified DBEs, MBEs, WBEs, VOSB and/or SDVOSBs to work on this project. Those contacted and their responses must be a part of the bidder's outreach efforts documentation.

7. Sent written notices, by certified mail, email, or facsimile, to qualified, certified small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs soliciting their participation in the contract not less than seven (7) days prior to the deadline for submission of bids to allow them to participate effectively.

8. Followed up initial solicitations by contacting small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs via tailored communications to determine their level of interest.

9. Provided the interested small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs with adequate and timely information about the plans, specifications, and requirements of the contract.

10. Selected portions of the work to be performed by small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs in order to increase the likelihood of subcontracting participation. This includes, where appropriate, breaking out contract work items into economically feasible units to facilitate small, DBE, MBE, WBE, VOSB and/or SDVOSB participation, even when the prime contractor may otherwise perform these work items with its own workforce.

11. Negotiated in good faith with interested small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs, not rejecting them as unqualified without sound reasons based on a thorough investigation of their capabilities. Any rejection must be so noted in writing with a description as to why an agreement could not be reached.

12. Included documentation of quotations received from interested small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs that were not used due to uncompetitive pricing or were rejected as unacceptable and/or copies of responses from firms indicating that they would not be submitting a bid.

    a. Bidder has to submit sound reasons why the quotations were considered unacceptable. The fact that the bidder has the ability and/or desire to perform the contract work with its own forces will not be considered a sound reason for rejecting a small business', DBE's MBE's, WBE's, VOSB's and/or SDVOSB's quote. Nothing in this provision shall be construed to require the bidder to accept unreasonable quotes in order to satisfy the participation goals.

13. Made an effort to offer assistance to or refer interested small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs to obtain the necessary equipment, supplies, materials, insurance and/or bonding to satisfy the work requirements of the bid proposal.

14. Made efforts to expand the search for small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs beyond the usual geographic boundaries.

15. Other – any other evidence that the bidder submits that may demonstrate that the bidder has made reasonable efforts to include small, DBE, MBE, WBE, VOSB and/or SDVOSB participation.

Bidder must document, with specificity, each of the efforts it made to include small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs as subcontractors in the procurement, including the date on which each effort was made, the medium through which each effort was made, and the outcome of each effort.

Note: Failure to submit the documentation requested in this section may be cause for rejection of bid. Bidders may include any other documentation deemed relevant to this requirement which is subject to review by the MBE Liaison. Documentation of Good Faith and Outreach Efforts must be submitted with the Bid, regardless of the proposed level of small, DBE, MBE, WBE, VOSB and/or SDVOSB participation in the procurement. If the Good Faith and Outreach Effort documentation is not submitted with the bid response, the bid may be rejected.

OUTREACH EFFORTS EVALUATION

Outreach efforts demonstrated by the bidder or respondent will be evaluated on a pass/fail basis.

ATTACHMENT A – SMALL AND DISADVANTAGED, MINORITY-, WOMEN-, AND VETERAN-OWNED BUSINESS OUTREACH PLAN

Proposer Name:	Strategic Communications, LLC	**Date:**	04/20/2026
Project Name:	RFP 12-2026 IT CONSULTING & TECH SERVICES	**Project Number:**	
Contact Name:	Paige Reh	**Telephone:**	502-493-7234/502-813-8048
Email:	preh@yourstrategic.com		

The mission of the Minority Business Enterprise Program is to facilitate the full participation of disadvantaged businesses, minority-, women-, veteran-, and service-disabled veteran-owned businesses in the procurement process and to promote economic inclusion as a business imperative essential to the long -term economic viability of Lexington-Fayette Urban County Government.

To that end, small and disadvantaged businesses, including minority-, woman-, veteran-, and service-disabled veteran-owned businesses, must have an equal opportunity to be utilized in the performance of contracts with public funds spent from certain discretionary agreements. By submitting its offer, Bidder/Proposer certifies that it has taken, and if there are further opportunities will take, reasonable steps to ensure that small and disadvantaged businesses, including minority-, woman-, veteran-, and service-disabled veteran-owned businesses, are provided an equal opportunity to compete for and participate in the performance of any subcontracts resulting from this procurement.

The information submitted in response to this clause will not be considered in any scored evaluation. Failure to submit this form may cause the bid or proposal to be rejected.

Is the Bidder/ Proposer a certified firm? Yes ☑ No ☐

If yes, indicate all certification type(s):

DBE ☐ MBE ☑ WBE ☑ SBE ☐ VOSB/SDVOSB ☐

and supply a copy of the certificate and/or certification letter if not currently listed on the city's Minority Business Enterprise Program's (MBEP) certified list.

1. Include a list of firms that Bidder/ Proposer has had a contractual relationship with within the last two years that are minority-owned, woman-owned, veteran-owned or small businesses, regardless of their certification status.

Click or tap here to enter text.

2. Does Bidder/Proposer foresee any subcontracting opportunities for this procurement?

Yes ☑ No ☐

If no, please explain why in the field below. Do not complete the rest of this form and submit this first page with your bid and/or proposal. Click or tap here to enter text.

If yes, please complete the following pages and submit all pages with your bid and/or proposal.

Describe the steps Bidder/Proposer took to solicit small and disadvantaged businesses, including MBEs, WBEs, VOSBs, and SDVOSBs, for subcontracting opportunities for this procurement.

3. Check the good faith and outreach efforts the Bidder/Proposer used to encourage the participation of small and disadvantaged businesses including, MBEs, WBEs, VOSBs and SDVOSBs:

- ☐ Bidder placed advertisements in search of prospective small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs for the solicitation.
- ☑ Bidder attended LFUCG Procurement Economic Inclusion Outreach event(s) within the past year.
- ☑ Bidder attended pre-bid and/or pre-proposal meetings for this solicitation.
- ☐ Bidder sponsored an Economic Inclusion Outreach event.
- ☐ Bidder requested a list of certified small, DBE, MBE, WBE, VOSB and/or SDVOSB subcontractors or suppliers from LFUCG.
- ☑ Bidder contacted organizations that work with small, DBE, MBE, WBE, VOSB and/or SDVOSB companies.
- ☐ Bidder sent written notices to certified small, DBE, MBE, WBE, VOSB and SDVOSB businesses.
- ☐ Bidder followed up to initial solicitations with interested small, DBE, MBE, WBE, VOSB and/or SDVOSB.
- ☐ Bidder provided small, DBE, MBE, WBE, VOSB and/or SDVOSB businesses interested in performing the solicited work with prompt access to the plans, specifications, scope of work, and requirements of the solicitation.
- ☐ Bidder made efforts to segment portions of the work to be performed by small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs, including dividing sub-bid/partnership opportunities into economically feasible units/parcels, to facilitate participation.

☑ Bidder negotiated in good faith with interested small, DBE, MBE, WBE, VOSB and/or SDVOSB businesses.

☐ Bidder provided adequate rationale for rejecting any small business', DBEs, MBEs, WBEs, VOSBs or SDVOSBs for lack of qualifications.

☐ Bidder offered assistance in obtaining bonding, insurance, financial, equipment, or other resources to small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs, in an effort to assist them in meeting project requirements.

☐ Bidder made efforts to expand the search for small businesses, DBEs MBEs, WBEs, VOSBs and/or SDVOSBs beyond the usual geographic boundaries.

☑ Bidder made other reasonable efforts to include small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs participation.

4. Bidder/Proposer must include documentation, including the date each effort was made, the medium through which each effort was made, and the outcome of each effort with this form, regardless of the level of small, DBE, MBE, WBE, VOSB and/or SDVOSB participation. Examples of required documentation include copies of email communications, copies of newspaper advertisements, or copies of quotations received from interested small businesses, DBEs, MBEs, WBEs, VOSBs or SDVOSBs.

Click or tap here to enter text.

For detailed information regarding outreach efforts that satisfy the MBE Program's requirements, please see "Documentation Required for Good Faith Efforts and Outreach Plans" page.

Note: The Bidder/Proposer must be willing to report the identity of each subcontractor and the value of each subcontract to MBEP if awarded a contract from this procurement.

Failure to submit the documentation requested may be cause for rejection of the bid. Bidders may include any other documentation deemed relevant to this requirement, which is subject to review by the MBE Liaison. Documentation of Good Faith and Outreach Efforts must be submitted with the bid, regardless of the proposed level of SBEs, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs participation in the procurement. If the Good Faith and Outreach Effort Form and associated documentation is not submitted with the bid response, the bid may be rejected.

The undersigned acknowledges that all information is accurate. Any misrepresentations may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and claims.

Strategic Communications, LLC	Paige Reh
Company	**Company Representative**
04/20/2026	Director of HR & Administration
Date	**Title**

4870-1925-6809, v. 1

Attachment F, General Provisions

GENERAL PROVISIONS

1. Each Respondent shall comply with all Federal, State & Local regulations concerning this type of service or good.

   The Respondent agrees to comply with all statutes, rules, and regulations governing safe and healthful working conditions, including the Occupational Health and Safety Act of 1970, *29 U.S.C. 650 et. seq.*, as amended, and KRS Chapter 338. The Respondent also agrees to notify the LFUCG in writing immediately upon detection of any unsafe and/or unhealthful working conditions at the job site. The Respondent agrees to indemnify, defend and hold the LFUCG harmless from all penalties, fines or other expenses arising out of the alleged violation of said laws.

2. Failure to submit ALL forms and information required in this RFP may be grounds for disqualification.

3. Addenda: All addenda and IonWave Q&A, if any, shall be considered in making the proposal, and such addenda shall be made a part of this RFP. Before submitting a proposal, it is incumbent upon each proposer to be informed as to whether any addenda have been issued, and the failure to cover in the bid any such addenda may result in disqualification of that proposal.

4. Proposal Reservations: LFUCG reserves the right to reject any or all proposals, to award in whole or part, and to waive minor immaterial defects in proposals. LFUCG may consider any alternative proposal that meets its basic needs.

5. Liability: LFUCG is not responsible for any cost incurred by a Respondent in the preparation of proposals.

6. Changes/Alterations: Respondent may change or withdraw a proposal at any time prior to the opening; however, no oral modifications will be allowed. Only letters, or other formal written requests for modifications or corrections of a previously submitted proposal which is addressed in the same manner as the proposal, and received by LFUCG prior to the scheduled closing time for receipt of proposals, will be accepted. The proposal, when opened, will then be corrected in accordance with such written request(s), provided that the written request is contained in a sealed envelope which is plainly marked “modifications of proposal”.

7. Clarification of Submittal: LFUCG reserves the right to obtain clarification of any point in a bid or to obtain additional information from a Respondent.

8. Bribery Clause: By his/her signature on the bid, Respondent certifies that no employee of his/hers, any affiliate or Subcontractor, has bribed or attempted to bribe an officer or employee of the LFUCG.

9. Additional Information: While not necessary, the Respondent may include any product brochures, software documentation, sample reports, or other documentation that may assist LFUCG in better understanding and evaluating the Respondent's response. Additional documentation shall not serve as a substitute for other documentation which is required by this RFP to be submitted with the proposal,

10. Ambiguity, Conflict or other Errors in RFP: If a Respondent discovers any ambiguity, conflict, discrepancy, omission or other error in the RFP, it shall immediately notify LFUCG of such error in writing and request modification or clarification of the document if allowable by the LFUCG.

11. Agreement to Bid Terms: In submitting this proposal, the Respondent agrees that it has carefully examined the specifications and all provisions relating to the work to be done attached hereto and made part of this proposal. By acceptance of a Contract under this RFP, proposer states that it understands the meaning, intent and requirements of the RFP and agrees to the same. The successful Respondent shall warrant that it is familiar with and understands all provisions herein and shall warrant that it can comply with them. No additional compensation to Respondent shall be authorized for services or expenses reasonably covered under these provisions that the proposer omits from its Proposal.

12. Cancellation: If the services to be performed hereunder by the Respondent are not performed in an acceptable manner to the LFUCG, the LFUCG may cancel this contract for cause by providing written notice to the proposer, giving at least thirty (30) days notice of the proposed cancellation and the reasons for same. During that time period, the proposer may seek to bring the performance of services hereunder to a level that is acceptable to the LFUCG, and the LFUCG may rescind the cancellation if such action is in its best interest.

A. Termination for Cause

(1) LFUCG may terminate a contract because of the contractor's failure to perform its contractual duties

(2) If a contractor is determined to be in default, LFUCG shall notify the contractor of the determination in writing, and may include a specified date by which the contractor shall cure the identified deficiencies. LFUCG may proceed with termination if the contractor fails to cure the deficiencies within the specified time.

(3) A default in performance by a contractor for which a contract may be terminated shall include, but shall not necessarily be limited to:
(a) Failure to perform the contract according to its terms, conditions and specifications;
(b) Failure to make delivery within the time specified or according

to a delivery schedule fixed by the contract;

(c) Late payment or nonpayment of bills for labor, materials, supplies, or equipment furnished in connection with a contract for construction services as evidenced by mechanics' liens filed pursuant to the provisions of KRS Chapter 376, or letters of indebtedness received from creditors by the purchasing agency;

(d) Failure to diligently advance the work under a contract for construction services;

(e) The filing of a bankruptcy petition by or against the contractor; or

(f) Actions that endanger the health, safely or welfare of the LFUCG or its citizens.

B. At Will Termination

Notwithstanding the above provisions, the LFUCG may terminate this contract at will in accordance with the law upon providing thirty (30) days written notice of that intent, Payment for services or goods received prior to termination shall be made by the LFUCG provided these goods or services were provided in a manner acceptable to the LFUCG. Payment for those goods and services shall not be unreasonably withheld.

13. Assignment of Contract: The contractor shall not assign or subcontract any portion of the Contract without the express written consent of LFUCG. Any purported assignment or subcontract in violation hereof shall be void. It is expressly acknowledged that LFUCG shall never be required or obligated to consent to any request for assignment or subcontract; and further that such refusal to consent can be for any or no reason, fully within the sole discretion of LFUCG.

14. No Waiver: No failure or delay by LFUCG in exercising any right, remedy, power or privilege hereunder, nor any single or partial exercise thereof, nor the exercise of any other right, remedy, power or privilege shall operate as a waiver hereof or thereof. No failure or delay by LFUCG in exercising any right, remedy, power or privilege under or in respect of this Contract shall affect the rights, remedies, powers or privileges of LFUCG hereunder or shall operate as a waiver thereof.

15. Authority to do Business: The Respondent must be a duly organized and authorized to do business under the laws of Kentucky. Respondent must be in good standing and have full legal capacity to provide the services specified under this Contract. The Respondent must have all necessary right and lawful authority to enter into this Contract for the full term hereof and that proper corporate or other action has been duly taken authorizing the Respondent to enter into this Contract. The Respondent will provide LFUCG with a copy of a corporate resolution authorizing this action and a letter from an attorney confirming that the proposer is authorized to do business in the State of Kentucky if requested. All proposals must

be signed by a duly authorized officer, agent or employee of the Respondent.

16. Governing Law: This Contract shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky. In the event of any proceedings regarding this Contract, the Parties agree that the venue shall be the Fayette County Circuit Court or the U.S. District Court for the Eastern District of Kentucky, Lexington Division. All parties expressly consent to personal jurisdiction and venue in such Court for the limited and sole purpose of proceedings relating to this Contract or any rights or obligations arising thereunder. Service of process may be accomplished by following the procedures prescribed by law.

17. Ability to Meet Obligations: Respondent affirmatively states that there are no actions, suits or proceedings of any kind pending against Respondent or, to the knowledge of the Respondent, threatened against the Respondent before or by any court, governmental body or agency or other tribunal or authority which would, if adversely determined, have a materially adverse effect on the authority or ability of Respondent to perform its obligations under this Contract, or which question the legality, validity or enforceability hereof or thereof.

18. Contractor understands and agrees that its employees, agents, or subcontractors are not employees of LFUCG for any purpose whatsoever. Contractor is an independent contractor at all times during the performance of the services specified.

19. If any term or provision of this Contract shall be found to be illegal or unenforceable, the remainder of the contract shall remain in full force and such term or provision shall be deemed stricken.

20. Contractor [or Vendor or Vendor's Employees] will not appropriate or make use of the Lexington-Fayette Urban County Government (LFUCG) name or any of its trade or service marks or property (including but not limited to any logo or seal), in any promotion, endorsement, advertisement, testimonial or similar use without the prior written consent of the government. If such consent is granted LFUCG reserves the unilateral right, in its sole discretion, to immediately terminate and revoke such use for any reason whatsoever. Contractor agrees that it shall cease and desist from any unauthorized use immediately upon being notified by LFUCG.

Signature _____ Date 4/14/2026

Attachment G, Insurance Coverage

STRACOM-01 WHIKA1

ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 3/18/2026

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER RISE Partners 908 Lily Creek Rd Ste 101 Louisville, KY 40243	CONTACT NAME: Kaylee Pasquale PHONE (A/C, No, Ext): FAX (A/C, No): E-MAIL ADDRESS: kaylee.white@riseptrs.com	
	INSURER(S) AFFORDING COVERAGE	NAIC #
INSURED Strategic Communications LLC 310 N. Evergreen Road Louisville, KY 40243	INSURER A : Hartford Fire Insurance Company	19682
	INSURER B : Trumbull Insurance Company	27120
	INSURER C : Hartford Casualty Insurance Company	29424
	INSURER D : Hartford Fire & Its P&C Affiliates	00914
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS		
A	X COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	$	1,000,000
	CLAIMS-MADE X OCCUR	X	X	33UUNBP2FCH	5/5/2025	5/5/2026	DAMAGE TO RENTED PREMISES (Ea occurrence)	$	100,000
							MED EXP (Any one person)	$	5,000
							PERSONAL & ADV INJURY	$	1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$	2,000,000
	POLICY X PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$	2,000,000
	OTHER:						EMPLOYEE BENEFI	$	1,000,000
B	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$	1,000,000
	X ANY AUTO			33UENBP2FCW	5/5/2025	5/5/2026	BODILY INJURY (Per person)	$	
	OWNED AUTOS ONLY / SCHEDULED AUTOS						BODILY INJURY (Per accident)	$	
	HIRED AUTOS ONLY / NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$	
								$	
C	X UMBRELLA LIAB X OCCUR						EACH OCCURRENCE	$	5,000,000
	EXCESS LIAB CLAIMS-MADE			33XHUBP2JB2	5/5/2025	5/5/2026	AGGREGATE	$	5,000,000
	DED RETENTION $							$	
D	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY						X PER STATUTE OTH-ER		
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N: Y	N/A		33WEBP2FCP	5/5/2025	5/5/2026	E.L. EACH ACCIDENT	$	1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$	1,000,000
							E.L. DISEASE - POLICY LIMIT	$	1,000,000
A	Errors & Omissions L			33 TE 0737311-25	5/5/2025	5/5/2026	Aggregate		5,000,000
A	Cyber Liability			33 TE 0737311-25	5/5/2025	5/5/2026	Aggregate		5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Broward County is additional insured for General liability. Insured's insurance shall provide primary coverage and shall not require contribution from the County, self-insurance or otherwise. Waiver of subrogation applies in favor of Broward County. .

CERTIFICATE HOLDER	CANCELLATION
Broward County 115 South Andrews Avenue Fort Lauderdale, FL 33301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE

ACORD 25 (2016/03)