# THE CITY OF OKLAHOMA CITY
# ADDENDUM NO. 1

## RFP25801
## PURCHASING CARD SERVICES

Prepared by:
The City of Oklahoma City
Procurement Services
Recommended for Approval – Sharmanlyne Vickers, Purchasing Agent

Sharmanlyne Vickers

The City of Oklahoma City is issuing Addendum No. 1 to RFP25801 – Purchasing Card Services to include Attachment A to the proposal documents. This addendum also extends the question and answer period to January 17, 2025 at 12:00:00 PM CST and the closing date to January 22, 2025 at 4:00:00 PM CST.

## CURRENT TECHNICAL ENVIRONMENT

## OVERVIEW

A centralized Information Technology (IT) department, in concert with departmental contacts, provides the City of Oklahoma City (The City) and its Trusts support for information systems. System standards are established and approved through a formal process. Deviation from standards **must** be approved in writing.

## NETWORK ENVIRONMENT

The City of Oklahoma City network design follows the Cisco Enterprise Scalable *Core – Distribution –Access* model incorporating Cisco and Industry Best-Practices whenever possible. End devices leverage Fast Ethernet or Gigabit switch ports. Network is provisioned with multicast to support streaming video/audio that is IGMP/CGMP sparse mode compliant.

The City of Oklahoma City has implemented a TCP/IP routed environment. TCP/IP is the only protocol permitted in the routed environments. All new systems are required to utilize DNS for name resolution and may not utilize broadcast-based naming resolution. DHCP with Dynamic DNS Update provisions the majority of IP addressing for end devices.

The City of Oklahoma City utilizes next generation firewalls with an explicit denial for all non-approved traffic traversing the DMZ into the City's internal networks. Traffic emanating from the public internet is only authorized to enter into a DMZ server and not directly into the City's internal networks. The City reserves the right to decrypt and perform deep packet inspection on all traffic traversing any network zone that is under our control. The City also reserves the right to monitor and log all internet usage.

City connectivity to vendor applications that require remote connection to off-site resources is accomplished by establishing an IPSEC tunnel. Vendors that choose to leverage this facility are required to work with the City Network and Security Teams and adhere to all City requirements to accomplish this mode of transport.

The City of Oklahoma City has established a structured wiring plan that requires the use of CAT6 cabling to RJ-45 wall jacks in a modular configuration: conductors from faceplate to MDF/IDF can transport either data or voice as required with discrimination implemented in the equipment closet by appropriate patch. Legacy wiring is CAT5. All additional wiring and equipment will comply with this plan unless specific, written authorization has been given by the Information Technology Department before installation.

Networks other than the City's will not be directly connected to the City of Oklahoma City network. For remote access to the network, The City has provisioned Virtual Private Network (VPN) services. This will be the only supported method to access systems within The City network unless specific, written authorization has been given by the Information Technology Department before installation.

## AUTHENTICATION REQUIREMENTS

- Our preference for authentication would be to use a SAML 2.0 SSO solution leveraging Microsoft Azure as the authentication provider.

- On premise applications could use LDAP based authentication if SAML 2.0 SSO via Microsoft Azure isn't available.

## SERVER ENVIRONMENT

The City servers are housed and managed in Tier 2 data centers with backup power, secure access control, and environmental control. The City uses commodity-based, non-proprietary hardware. The architecture is redundant, scalable, and a multi-tiered server environment. The City prefers to use the most current Windows operating system with all updates applied. Server virtualization compatibility is highly preferred. The City currently uses Active Directory domain.

The City employs an aggressive patching policy for all Servers. Patches that are related to security issues start the testing process the day of release and are moved to production servers on a defined schedule. Vendors supplying applications to the City must be compatible with current and future OS patching and notify the City of any issues the current patches cause with their application within 10 business days of the operating system patches release. Any incapability with OS patching must be corrected within 30 days.

## TECHNICAL PREFERENCES

### GENERAL

The City desires to acquire a system that streamlines and enhances its Practice Management business processes. Those objectives can only be reached by implementing a new system that includes the following minimum attributes:

- An application that includes the functionality required by departments to conduct their business efficiently and effectively.
- An application that is made available to the user within a secure technical environment that has: availability, accessibility, flexibility, maintainability, stability, expandability, capacity, and responsiveness.

In addition to providing the functionality defined within the prior sections, the City also requires the Proposer to fully describe the technical environment envisioned for the City in order to achieve its stated objectives.

The City anticipates purchasing any additional servers, networking components, desktop systems, and associated system software through existing contracts. Proposers may include such items as alternates for consideration; however, all specifications, unit pricing, discount pricing, installation, and warranty information must be clearly provided and described.

Regardless of how the required hardware and system software is purchased, the Proposer must accept responsibility for defining the technical requirements and associated configuration required to meet the City's stated objectives.

### GENERAL PREFERENCES

The City does not wish to discourage creative solutions nor stifle effective competition. Consequently, various technical architectures and system environments will be seriously considered and evaluated. There will, however, be certain expectations and preferences that will guide the evaluation process.

## NETWORKING PREFERENCES

The City's networking infrastructure is maintained and managed solely by City personnel. Proposers must take responsibility for specifying the requirements necessary for network communications as required to successfully implement the proposed system(s). To that end, the following concepts should be observed:

- The City's network configurations and components are not generally accessible to vendors. Vendors will not be allowed to monitor, configure, or add network components to the existing infrastructure without prior written permission.
- The vendor may propose additional network expansion or may instead choose to identify capacity requirements between devices to leverage existing infrastructure. Proposals for both approaches can be submitted for consideration.
- Vendors must specify bandwidth requirements between clients and servers, as well as between the various servers.
- Vendor is expected to define the required interface / connection between wireless data infrastructure and the City network. This should include, but not be limited to, explanations of client-side software requirements, supported operating systems, device options, and bandwidth requirements. Wi-Fi networks, even owned by the City, are treated as "foreign networks" and will be subject to firewall controls. Applications should be "Wi-Fi aware": capable of queuing both the server and client side of transactions.
- Vendor must specify proposed demarcation of responsibilities between the City and the vendor prior to system installation, testing, warranty, and maintenance.
- Remote vendor support of application will leverage the City maintained VPN solution. Modems are not permitted in the City network infrastructure.

## SERVER/DESKTOP PREFERENCES

Proposer must specify both the minimum and recommended hardware configurations for Servers, Clients, and Network paths required to operate the application at the required service and performance levels. Proposers may assume no competing load for the purpose of the specification.

**Server/Desktop preferences are as follows:**

- In general, there is a preference for commodity-based, non-proprietary hardware. Any departure from this will require extensive justification.
- Architectural preference is for a redundant, scalable, multi-tiered, multi-server environment.
- Preference is for a common shared backup management, logging, and recovery environment.
- The City utilizes an enterprise grade server management platform for administration, maintenance and logging.
- Operating System preference is currently Windows Server 2019.
- Relational database management system preference is Microsoft SQL Server 2019 or higher.
- The expectation is for a high-capacity, high-speed, redundant online disk storage subsystem. We would prefer to leverage this storage system if it is economically feasible for this implementation.
- The City uses Exchange Online as its messaging and collaboration system.
- The primary desktop and laptop client is an Intel-based system, with Windows operating systems. Currently most of the clients are running 64-bit Windows 11 operating system. The City's client PCs that have been purchased over time include many different processor speeds and other hardware combinations, so Proposers must specify the minimum required client configuration. New desktops being purchased are 4.5 GHz processors, 16 GB RAM, 256GB SSD, 64-bit Windows 11 Operating System, and

Microsoft Office 365. Mobile broadband in 4G or 5G may exist for some client systems.
- Ability for application packaging and distribution is highly preferred.
- Server virtualization compatibility is highly preferred and accomplished using Microsoft Hyper-V.
- SharePoint Online is our primary "intranet" and document storage solution.
- Power BI and SQL Server Reporting Services are our primary dashboard and reporting tools.

## DATA INTEGRATION PREFERENCES

Software vendors should adhere to the following standards to ensure that their solutions are interoperable with other systems and provide a high level of performance and security:

- Software vendors should provide industry-standard APIs for data integration that support multiple data formats and protocols, such as REST, SOAP, OData, JSON, and XML.
- Software vendors should provide comprehensive API documentation including, but not limited to, all endpoints, query parameters, request/response format, rate limiting, authentication and authorization mechanism, error codes, and examples of how to use the API.
- Software vendors should adhere to industry-standard data modeling standards, such as Common Data Model (CDM), to ensure that the data is well-structured and can be easily integrated with other systems.
- Software vendors should follow industry-standard security protocols, such as SSL/TLS encryption, to ensure that data is transmitted securely and protected from unauthorized access.

## SECURITY REQUIREMENTS FOR SaaS AND CLOUD APPLICATIONS

This City of Oklahoma has security requirements specifically targeting Software as a Service (SaaS) and cloud applications. These requirements are designed to ensure the protection of sensitive data and adherence to best security practices. Vendors must meet or exceed these standards to be considered for this project.

### Data Protection and Privacy

To ensure the highest level of data protection and privacy for SaaS and cloud applications, the following measures must be implemented by the vendor:
Encryption:

- Data at Rest: All data at rest must be encrypted using robust encryption standards such as AES-256.
- Data in Transit: Data in transit must be encrypted using TLS 1.2/1.3 or equivalent protocols.
- Data Residency: The data must be stored and processed within the continental United States, ensuring compliance with local data residency and sovereignty laws.

### Access Control and Identity Management

To manage access control and identity management effectively in SaaS and cloud applications, the vendor must adhere to the following requirements:
Authentication:

- Multi-Factor Authentication (MFA): MFA must be mandated for all user access to the cloud application.

- Single Sign-On (SSO): The solution must support SSO to integrate with existing identity management system (Azure Entra ID), such as SAML or OAuth.

Authorization:

- Role-Based Access Control (RBAC): RBAC must be implemented to ensure users have the minimum necessary access.
- Least Privilege Principle: The system must support the principle of least privilege for all users and services.

**Security Monitoring and Incident Response**

To ensure ongoing security and effective incident response for SaaS and cloud applications, the vendor must meet the following requirements:

Monitoring and Logging:

- Security Information and Event Management (SIEM): Integration with existing SIEM (Azure Sentinel) solutions for continuous monitoring is required.
- Log Management: Detailed logging of access and activity with tamper-evident logs is mandatory.

**Two-Way Radios: Current Environment**

The Oklahoma City (OKC) two-way radio environment features the advanced P25 Trunked Radio System, designed for enhanced public safety and emergency response. Key attributes include:

- **Dual-Phase Operation:** Supports both Phase 1 and Phase 2 communications.
- **Extensive Coverage:** 13 sites with linear simulcast technology ensure reliable communication across OKC and remote areas.
- **Dedicated RF Channels:** 20 channels optimized for high-demand and emergency situations.
- **Resilience:** Built to withstand EF-5 tornadoes, with diesel generators and DC power systems for extended outages.
- **Interoperability:** Communicates across 800 MHz bands for multi-agency operations.
- **Testing:** Regular computer-based drive testing ensures 99% reliability for handheld devices.
- **Capacity:** 38 simultaneous conversations supported by Phase 2 TDMA technology.
- **Active Talk Groups:** 601 groups for tactical, operational, and administrative communications.

**Technical Preferences**: Non-Public Safety Handheld Radios

- **Dimensions:** 5.9 x 2.4 x 1.9 inches, weight 10.9 oz.
- **Environmental Resistance:** Humidity, vibration, drop shock, IP66, and temperature range from -22°F to +140°F.
- **Frequency Range:** 700/800 MHz bands.
- **Digital Operation:** P25 protocol with AMBE+2 vocoding.
- **Battery:** Li-Ion, 3100 mAh, 10 hours life.

**Public Safety Handheld Radios**

- **Dimensions:** Similar to non-public safety, color: black.
- **Environmental Resistance:** Includes IP68 immersion, vibration, and temperature shock.
- **Frequency Range:** 700/800 MHz bands.
- **Digital Operation:** P25 protocol with AMBE+2 vocoding and ProVoice™.
- **Battery:** Li-Ion, 3100 mAh, 10 hours life.

**Public Safety and Non-Public Safety Single Band Mobile Radios**

- **Dimensions:** Standard mobile unit size with front-mount control.
- **Environmental Resistance:** IP54 protection, operational temperature from -22°F to +140°F.

- **Frequency Range:** 700/800 MHz.
- **Digital Operation:** Supports P25 Phase 1 and 2, and conventional analog modes.
- **Secure Communications:** 256 AES encryption.

**Special Purpose Multi-Band Mobile Radios**

- **Dimensions:** Varies for radio and control units.
- **Weight:** 5 to 7 lbs.
- **Channel Capacity:** 12,500 channels.
- **Environmental Resistance:** IP65 for control unit, IP54 for radio.
- **Frequency Range:** VHF, UHF, 700/800 MHz, 900 MHz.
- **Digital Operation:** P25 and ProVoice™ with multiple-key 256 AES encryption.

**Desktop Base Station Radios**

- **Standards:** Currently under development.

**Dispatch Consoles**

- **Processor:** Intel® Dual Core™ i7.
- **OS:** Windows® 10 Enterprise 64-bit.
- **Dimensions:** 1.75 x 16.75 x 10.5 inches.
- **Input Voltage:** 110-240 VAC.
- **External Interfaces:** Ethernet, USB, audio inputs/outputs.
- **Video:** DisplayPort connections for up to 4 monitors.
- **Storage:** Removable SSD.

**Conventional Base Stations/Repeaters**

**Standards:** Currently under development.

**RATIFIED** and **APPROVED** by the City Council of The City of Oklahoma City and **SIGNED** by the Mayor this 6TH day of MAY, 2025.

ATTEST:

Amy K. Simpson

CITY CLERK

SEAL OF THE CITY OF OKLAHOMA CITY

David Holt

MAYOR