CITY OF
ISLE
OF
PALMS South Carolina

From the Office of the Deputy City Administrator

MEMORANDUM for Record, Addendum seven (7) 21 August 2026

TO: All Prospective Bidders

FROM: Sean H. Kuester, Deputy City Administrator

C: N/a

RE: RFP 2026.09 “Managed IT Services”

**Note:** While the City would like to answer all questions, it will not directly reply to a question when doing so would create a vulnerability, reveal in great detail security measures or otherwise provide an advantage to a bad actor. For these sorts of questions, the City will provide generalized responses sufficient for proposal purposes without increasing cybersecurity or operational risk.

**Question 1**: Please clarify the City's preferred initial contract term and anticipated renewal structure. While Addendum 3 states that the term will be negotiated and that the City envisions a multi-year agreement, should contractors price their proposals assuming a three-year initial term, or should pricing be presented on an annual basis independent of contract term?

**Answer 1**: For proposal and pricing purposes, proposers should assume a three-year initial term with up to two additional one-year renewal periods, for a total potential term not to exceed five years. Pricing should be presented separately for Years 1, 2, and 3, with any annual escalation clearly identified. Proposers may also provide pricing or escalation assumptions applicable to renewal Years 4 and 5. Any renewal would be subject to satisfactory performance, required City approvals, mutual agreement of the parties, and availability and appropriation of funds.

Proposers may also identify any pricing incentives, discounts, or other considerations that would apply if the City elects to enter into a term longer than three years.

POST OFFICE DRAWER 508
ISLE OF PALMS, SOUTH CAROLINA 29451

843.886.6428
skuester@isleofpalms.gov
www.iop.net

**Question 2**: Please clarify the City's expected onsite response time for routine, urgent, and critical incidents. The RFP requires onsite support as required but does not establish a specific onsite response-time SLA.

**Answer 2**: The City has not established a specific mandatory onsite response-time SLA for routine, urgent, or critical incidents as part of this RFP.
As stated in Addendum 3, proposers should clearly describe their onsite support model, including the location of personnel responsible for onsite response and their anticipated response times. Proposers should identify their proposed service levels for routine, urgent, and critical incidents and distinguish, where applicable, between initial response, remote technical response, and onsite response.

The City expects response times to be appropriate to the severity and operational impact of the incident. Critical incidents affecting public safety, cybersecurity, continuity of government, or essential municipal operations require priority response consistent with the critical-incident examples provided in Answer 16 of Addendum 3.

The ability to provide timely onsite support, including during emergencies and after normal business hours when required, will be considered as part of the City's evaluation of the proposer's service delivery and operational support capabilities.

**Question 3**: Please clarify the expected response and restoration/mitigation targets for after-hours critical incidents, including whether the City expects 24x7x365 live response or an on-call response model.

**Answer 3**: The City expects 24x7x365 availability for response to critical incidents as defined in Answer 16 of Addendum 3. The City does not require a continuously staffed 24x7 general help desk, and an on-call support model is acceptable provided it results in timely live engagement by qualified technical personnel when a critical incident occurs. The required after-hours response to critical incidents described above is part of Base Monthly Support. Any separately stated after-hours rate would apply to authorized services outside the Base Monthly Support scope.

Critical incidents should receive immediate priority, with active triage, containment, mitigation, or development of a reasonable workaround beginning as promptly as practicable and continuing until the affected critical service is restored or the incident has been stabilized and an acceptable interim solution is in place.

The City has not established specific numerical response or restoration-time SLAs as part of this RFP. Proposers should clearly identify their proposed service levels for after-hours critical incidents, including:

- Initial acknowledgment or live response;
- Engagement by qualified technical personnel;
- Escalation procedures;
- Target time to mitigation, containment, or workaround; and
- Target time to restoration, where reasonably capable of being established.

The City recognizes that restoration times may vary based upon the nature of the incident, third-party dependencies, equipment availability, cybersecurity considerations, and other circumstances outside the provider's direct control.

For cybersecurity services, proposers should also note that the City's current environment includes 24x7x365 security monitoring and incident response, as described in Addendum 6.

**Question 4**: Please clarify whether unlimited help desk support includes unlimited onsite labor and travel, or whether the base monthly fee is intended to cover remote/telephone support with onsite labor and/or travel billed separately under the professional-services pricing structure.

**Answer 4**: The Base Monthly Support fee is intended to include unlimited help desk support by remote, telephone, and onsite means as reasonably required to perform services that fall within the Base Monthly Support scope.

Accordingly, routine onsite labor and ordinary travel necessary to troubleshoot or resolve an issue that is otherwise within the Base Monthly Support scope should be included in the base monthly fee and should not be separately billed solely because onsite service is required.

“Unlimited help desk support” should not be interpreted to mean that all onsite work of any nature is included in the base fee. Services identified in the RFP as Professional Services Outside Base Monthly Support—including major projects, implementations, migrations, infrastructure refreshes, and extended onsite emergency operations—may be separately priced and require City authorization, regardless of whether that work is performed remotely or onsite.

Travel associated with separately authorized professional services may be separately billed in accordance with the proposer's stated pricing methodology. Proposers should clearly identify any assumptions or exceptions affecting these pricing arrangements.

**Question 5**: For onsite support provided by an out-of-state proposer, should travel expenses, lodging, rental vehicles, airfare, mileage, and related travel time be included within the base monthly fee or billed separately at the proposer's published travel rates?

**Answer 5**: For routine onsite support that falls within the Base Monthly Support scope, proposers should include within their base monthly fee the labor, travel time, transportation, lodging, mileage, airfare, rental vehicle costs, and other travel-related expenses necessary to provide the required onsite service. Such costs should not be separately billed to the City solely because the proposer elects to provide the service using personnel located outside the immediate area.

The City does not provide a preference based solely on a firm's geographic location; however, each proposer is responsible for structuring its staffing and service-delivery model in a manner that satisfies the onsite support and response requirements of the RFP.

For separately authorized Professional Services, major projects, extended emergency operations, or other work specifically identified as outside Base Monthly Support, reasonable travel time and travel-related expenses may be separately billed if clearly identified in the proposer's pricing methodology and authorized by the City. Proposers should clearly identify any applicable travel rates, reimbursable expenses, limitations, or other assumptions in their Detailed Pricing Proposal.

**Question 6**: For hurricane and declared-emergency support, does the City anticipate a standby model in which personnel are pre-positioned or placed on call before an event, and if so, should standby/pre-staging costs be included in the base fee or separately priced?

**Answer 6**: As stated in Answer 13 of Addendum 3, the City is receptive to proposers describing their recommended emergency support model, including pre-staging, standby, activation, and post-event support.

The City does not require personnel to be physically pre-positioned for every hurricane or declared emergency. Every contingency will be conditions-based. Depending upon the nature and anticipated impact of an event, the City's emergency support posture may include priority remote support, qualified personnel placed on call, pre-event coordination, onsite support when conditions permit and it is safe to do so, and, when warranted, pre-positioning or dedicated support personnel.

Routine emergency preparedness, priority support, and the operational support contemplated in the Base Monthly Support section of the RFP before, during, and after significant events such as hurricanes should be included in the base monthly fee.

If a proposer recommends dedicated pre-staging, personnel specifically reserved for standby, extended onsite support, prolonged Emergency Operations Center activation, multi-day disaster response, or other services beyond the Base Monthly Support scope, those services may be separately priced. Proposers should clearly identify the applicable rates, activation criteria, minimum charges, travel costs, and other pricing assumptions associated with those services.

Any separately billed emergency standby, pre-staging, or extended support services would be subject to City authorization.

**Question 7**: Should proposers include EDR, SOC monitoring, email security, vulnerability management, phishing protection, and related cybersecurity tooling within the base monthly fee, or should these be presented as separately priced technology components?

**Answer 7**: The cybersecurity functions identified in the Base Monthly Support section of the RFP—including endpoint detection and response (EDR), security monitoring, vulnerability detection and remediation, MFA administration, email protection, phishing response, and security event monitoring—are required components of the City's base managed services solution.

Proposers should include the services and technology necessary to provide those required capabilities in their proposed recurring solution. The City recognizes that firms may structure pricing differently. Accordingly, a proposer may either include the associated cybersecurity licensing and tooling within its base monthly managed services fee or separately itemize those technology costs for pricing transparency.

If cybersecurity licenses, subscriptions, SOC services, or other required technology components are separately itemized, they should be clearly identified as mandatory recurring components of the proposed base solution and not presented as optional services. The City will consider those required components as part of the total recurring cost of the proposed managed services solution.

Optional or enhanced cybersecurity services beyond the requirements of the RFP may be separately identified and priced.

As previously stated, the City is not requiring continuation of any particular cybersecurity product or manufacturer. Proposers should identify their recommended solutions and clearly disclose any implementation, migration, one-time, or recurring costs associated with those recommendations.

**Question 8**: Should proposers include existing Microsoft licensing costs in the base monthly managed-services fee, or should Microsoft licensing be treated as a pass-through/variable cost based on actual licenses?

**Answer 8**: The Base Monthly Support fee should include the administration and management of the City's Microsoft 365 environment and licensing, as described in the RFP and Addendum 6.

The actual cost of Microsoft licenses and subscriptions should be separately identified and treated as a variable or pass-through technology cost based upon the City's actual authorized licensing quantities and subscription levels rather than embedded within the base managed-services fee.

Proposers should clearly identify their proposed licensing methodology, including any reseller discounts, administrative fees, markups, minimum commitments, annual terms, or other assumptions affecting Microsoft licensing costs.

Changes in license quantities, license types, upgrades, or other material subscription changes would be subject to City authorization. The City expects the selected provider to periodically review the City's licensing and recommend opportunities to consolidate, right-size, or otherwise reduce costs where appropriate.

**Question 9**: Please confirm whether the initial pricing baseline should remain 50 managed users and 82 email-only users throughout the initial contract period, with per-user pricing applied to increases/decreases, or whether the City expects periodic reconciliation of actual user counts.

**Answer 9**: For proposal and evaluation purposes, proposers should use 50 Managed Users and 82 Email-Only Users as the initial pricing baseline.
As stated in Addendum 3 and Addendum 5, these counts are estimates and may increase or decrease during the contract term. The City anticipates that actual user counts will be periodically reconciled and that applicable per-user charges will adjust accordingly based upon the number and type of users then being supported.

Proposers should clearly identify their proposed methodology for reconciling user counts, including the timing of adjustments, any minimum quantities or pricing thresholds, treatment of users added or removed during a billing period, and any volume discounts.

The quantities of 50 Managed Users and 82 Email-Only Users should not be interpreted as guaranteed minimum billable quantities for the entire contract term unless otherwise agreed during contract negotiations.

**Question 10**: Please clarify whether the base monthly fee is expected to include all monitoring and management software required to support the approximately 90 workstations, nine (9) servers, network infrastructure, firewalls, backup environment, and Microsoft 365 environment.

**Answer 10**: The Base Monthly Support fee should include the monitoring, management, remote-support, patch-management, ticketing, and similar tools that the proposer ordinarily requires to perform the managed services identified in the RFP. Proposers should not separately charge the City for internal management tools or software agents necessary for the proposer to deliver the Base Monthly Support scope.

This should not be interpreted to require the base monthly managed-services fee to include every underlying third-party technology license, subscription, or platform used by the City. Microsoft licensing, third-party business applications, existing backup platform costs, and other separately licensed or contracted technology may be separately identified as applicable.

Where a technology component is necessary to satisfy a required Base Monthly Support capability, such as EDR, security monitoring, or other required cybersecurity functionality, proposers should clearly identify whether the associated technology cost is included within the base managed-services fee or separately itemized as a required recurring component of the proposed solution.

With respect to the City's existing backup environment, the RFP requires backup and disaster-recovery monitoring, periodic restore testing, and an annual disaster-recovery

exercise as part of Base Monthly Support. Proposers should not assume that the RFP requires immediate replacement of the City's existing backup platform or subscription. Proposers should clearly identify all required recurring technology costs, licensing assumptions, and any separately priced components necessary to provide their proposed solution.

**Question 11**: Please clarify the expected level of support for third-party applications such as BS&A, Axon, ImageTrend, PowerDMS, Geothinq, iWorks, and Diverse. Is the contractor expected to provide application administration, troubleshooting/vendor coordination only, or both?

**Answer 11**: For third-party applications such as BS&A, Axon, ImageTrend, PowerDMS, Geothinq, iWorks, Diverse, and similar systems, the Base Monthly Support scope is intended to include reasonable technical troubleshooting and vendor coordination necessary to support City operations and resolve incidents.

The selected provider should assist in identifying whether an issue originates with the City's workstation, network, server, Microsoft 365 environment, authentication, connectivity, or other supported infrastructure and, when appropriate, coordinate with the applicable software vendor through resolution.

The RFP does not require the managed-services provider to assume full application-specific administration, configuration, business-process management, or functional support for every third-party application unless such responsibilities are specifically identified and agreed upon by the City.

If a proposer recommends providing additional application administration or specialized support beyond routine troubleshooting and vendor coordination, those services should be clearly described and separately identified where they would result in additional cost.

**Question 12**: Please clarify whether the selected vendor's personnel who provide support to Police/Fire systems or access CJIS-related information must individually maintain CJIS security awareness/training, background checks, fingerprinting, or other CJIS personnel requirements, and whether the City will facilitate required access.

**Answer 12**: Yes. Vendor personnel whose duties require access to Criminal Justice Information (CJI), or privileged access to systems or networks through which CJI may be accessed, must satisfy all applicable CJIS Security Policy and South Carolina CJIS/SLED personnel-security requirements before such access is granted.

Depending upon the individual's duties and level of access, these requirements may include CJIS security awareness or role-based training, fingerprint-based criminal history record checks, required acknowledgments or agreements, and any other applicable access or certification requirements.

The requirement is based upon the nature and level of access rather than merely assignment to Police or Fire support. Personnel who do not access CJI and whose

duties do not provide access to systems or environments through which CJI may be accessed would not be subject to CJIS personnel requirements solely because they provide support to a public safety department.

The City, through the appropriate City and Police Department personnel and applicable SLED/CJIS processes, will coordinate the agency-side steps necessary to authorize appropriate vendor personnel. The selected provider will be responsible for ensuring that its personnel timely complete and maintain all applicable training, screening, documentation, and other eligibility requirements and shall not permit personnel to access CJI or CJIS-related systems until the required authorization has been obtained. Proposers should describe their experience supporting CJIS-regulated environments and their process for maintaining qualified personnel available to support the City's CJIS-related systems.

**Question 13**: Please clarify whether annual strategic planning, executive advisory services, technology roadmaps, budget planning, and capital planning are included in the base monthly fee or should be priced as professional services

**Answer 13**: The RFP distinguishes between routine executive-level advisory support associated with the ongoing managed-services relationship and formal strategic planning services.

The Base Monthly Support fee should include the Quarterly Operational Review identified in the RFP, routine executive consultation regarding the City's existing technology environment, operational recommendations, identification of emerging risks or needs, and other advisory support reasonably associated with managing the City's day-to-day technology environment.

As specifically identified under “Professional Services (Outside Base Monthly Support),” formal Annual Strategic Planning should be separately priced. This includes technology roadmap development or a “Greenfield” assessment, budget planning and forecasting, capital and replacement planning, asset portfolio assessments, and significant network redesign or architecture planning.

Proposers should clearly identify their pricing methodology for these Professional Services and describe what level of routine executive advisory support is included within the base monthly fee. Separately priced Professional Services would be performed with City authorization.

**Question 14**: Please clarify whether the quarterly executive operational review is expected to be conducted on-site or virtually.

**Answer 14**: The City has not prescribed a specific format for the Quarterly Operational Review. The review may be conducted onsite or virtually, provided the format supports meaningful engagement with City leadership and adequately addresses the operational, infrastructure, cybersecurity, asset lifecycle, and other matters identified in the RFP.

Proposers should describe their standard approach to quarterly executive reviews, including whether they typically conduct them onsite, virtually, or through a combination of both.

**Question 15**: Please clarify the expected transition period and whether the incumbent provider will be required to cooperate with knowledge transfer, credential transfer, documentation transfer, configuration transfer, and introduction of ONSI personnel.

**Answer 15**: The City has not established a fixed transition period. As stated in Answer 11 of Addendum 3, proposers should describe their recommended transition methodology, including key milestones, sequencing, timelines, dependencies, and risk mitigation measures. The City is open to a phased transition where doing so reduces operational risk and improves continuity of service. The final transition schedule will be developed and approved with the selected proposer.

The City anticipates reasonable cooperation from the incumbent provider during the transition and will facilitate coordination among the City, the incumbent provider, and the selected proposer as appropriate.

Proposers should identify any information, access, incumbent-provider coordination, or other dependencies they believe will be necessary to execute their proposed transition plan successfully.

**Question 16**: Will the City permit the selected provider to implement its standard ITSM/ticketing platform, including remote-management and endpoint-management agents, on City systems?

**Answer 16**: Deployment of such tools will be coordinated with and subject to City approval during transition. Proposed tools must be compatible with the City's environment, comply with applicable cybersecurity and CJIS requirements, and must not interfere with City systems, third-party applications, or separately contracted technology services that remain in place. As stated in Answer 6 of Addendum 3, the City is open to the selected provider implementing its standard IT service management (ITSM)/ticketing platform, provided it satisfies the City's operational requirements described in that answer.

The selected provider may also deploy its standard remote monitoring and management (RMM), endpoint-management, remote-support, patch-management, and similar software agents on City-managed systems where reasonably necessary to perform the Base Monthly Support scope.

**Question 17**: Please provide the current patch compliance rate across all endpoint and server categories reviewed during the engagement. Identify any systems operating on end-of-life or unsupported operating system versions. Confirm whether DISA Security Technical Implementation Guides (STIGs) or CIS Benchmarks serve as the active configuration baseline standard — and for any systems found to be out of compliance, describe the deviation, the risk accepted or mitigated, and the timeline for remediation.

**Answer 17**: The City will not publish detailed information regarding its current patch-compliance rates, specific unsupported or end-of-life systems, security configuration deviations, accepted cybersecurity risks, vulnerability findings, or remediation schedules as part of a public addendum.

As stated in prior addenda, the selected provider will receive additional technical information reasonably necessary to support transition and ongoing operations, subject to appropriate confidentiality and security requirements. The selected provider will be expected to validate the City's asset inventory, operating-system and patch status, security posture, and other relevant technical conditions during transition and to recommend appropriate remediation where necessary.
As previously stated in Addendum 3, the City has not formally adopted a single enterprise cybersecurity framework. The City requires compliance with applicable federal, state, local, CJIS, and other security requirements and expects cybersecurity practices consistent with recognized frameworks such as the NIST Cybersecurity Framework and applicable NIST publications.

The City has not established DISA STIGs or CIS Benchmarks as a universal configuration baseline for purposes of this RFP. Proposers should describe the secure-configuration and system-hardening standards they recommend for the City's environment and how they would address systems subject to particular regulatory or operational requirements.

**Question 18**: Confirm whether multi-factor authentication (MFA) is enforced at all remote access points and administrative interfaces. Identify the date of the most recent formal privileged access review, the methodology used, and whether any orphaned, stale, or over-permissioned accounts were identified and subsequently revoked or remediated.

**Answer 18**: The City will not publish detailed information regarding the configuration or coverage of its multi-factor authentication controls, privileged administrative interfaces, privileged account inventories, access-review findings, identified account deficiencies, or related remediation activities in a public addendum.

The RFP requires MFA administration and appropriate cybersecurity controls as part of Base Monthly Support. The selected provider will be expected during transition to review and validate identity and access-management controls, including MFA coverage, privileged access, administrative accounts, stale or inactive accounts, and other relevant access-security conditions, and to recommend or implement appropriate remediation where necessary.

The City expects the selected provider to maintain sound privileged-access-management practices consistent with applicable CJIS requirements, recognized cybersecurity frameworks, and industry best practices.

Additional technical information reasonably necessary to perform this review will be made available to the selected provider subject to appropriate confidentiality and security requirements.

**Question 19**: Please describe your current incident response capability in writing. Confirm whether a formal Incident Response Plan (IRP) is in place, the date it was last updated, and the date it was last tested or exercised — including the type of exercise conducted (tabletop, functional, full-scale). Describe the chain-of-custody procedures currently governing digital evidence collection and preservation and identify the personnel role(s) authorized to initiate evidence collection procedures and invoke the IRP.

**Answer 19**: As previously stated in Addendum 6, the City currently receives 24x7x365 cybersecurity monitoring and incident-response services through its incumbent managed service provider.

The City will not publish detailed incident-response procedures, internal escalation or activation protocols, digital-evidence collection procedures, chain-of-custody processes, authorized personnel roles, or other operational security information in a public addendum. The City also is not providing detailed information regarding the dates, scope, or results of prior incident-response reviews, tests, or exercises as part of this procurement.

The selected provider will be expected during transition to review the City's existing cybersecurity incident-response capabilities and documentation and to identify any recommended improvements necessary to establish or maintain an effective, current, and appropriately tested incident-response capability.

The selected provider must be capable of supporting cybersecurity incidents, including appropriate escalation, containment, preservation of relevant logs, coordination of appropriate digital-evidence preservation with authorized City/law-enforcement personnel or qualified specialists as required, and compliance with applicable CJIS and other legal or regulatory requirements.

Proposers should describe their own incident-response capabilities, escalation model, digital-forensics and evidence-preservation practices, and experience assisting governmental clients with incident-response planning and exercises. Additional City-specific technical or operational information reasonably necessary for these activities will be provided to the selected provider subject to appropriate confidentiality and security requirements.

**Question 20**: Please describe the current state of network micro-segmentation within the Isle of Palms environment. Confirm whether a formal Zero Trust Architecture (ZTA) implementation initiative is underway and the designated lead responsible for ZTA roadmap ownership and execution.

**Answer 20**: The City will not publish detailed information regarding its current network segmentation, micro-segmentation, trust boundaries, security zones, or related network architecture in a public addendum.

As previously stated, the City has not formally adopted a single enterprise cybersecurity framework. The City has not prescribed Zero Trust Architecture (ZTA) as a specific mandatory architecture or implementation requirement for purposes of this RFP. The selected provider will be expected during transition and ongoing strategic planning to review the City's network and cybersecurity architecture and identify appropriate opportunities for improving segmentation, access controls, security architecture, and organizational resilience.

Any recommended formal Zero Trust initiative, material network redesign, or significant architecture change would be evaluated by the City as part of its strategic technology planning and, where applicable, separately authorized consistent with the Professional Services provisions of the RFP.

Proposers should describe their experience with network segmentation and Zero Trust principles and may identify recommendations they believe would be appropriate for a municipal environment such as the City's. Additional City-specific network and security information reasonably necessary for such evaluation will be provided to the selected provider subject to appropriate confidentiality and security requirements.

**Question 21**: Will a proposer have to maintain any cameras?

**Answer 21**: The selected provider will not be expected to perform routine maintenance, repair, installation, or replacement of surveillance cameras or other physical camera-system equipment as part of the Base Monthly Support scope.

To the extent camera or video systems rely upon City-managed network infrastructure, servers, connectivity, or other technology that falls within the managed-services scope, the selected provider may be expected to provide reasonable technical troubleshooting and vendor coordination related to those supported components.

Specialized camera-system administration, maintenance, installation, replacement, or expansion would be handled separately or through the appropriate third-party provider unless specifically authorized by the City as an additional service.

**Question 22**: How many peripherals (iPads, Tablets, etc.) would need to be managed?

**Answer 22**: The City does not have a separately verified and up-to-date count of iPads, tablets, and similar mobile devices available for proposal purposes at this time. Based on legacy documentation, proposers may use 25–35 devices as a reasonable planning factor for proposal purposes. This figure is an estimate and should not be interpreted as a guaranteed or verified device count. The selected provider will be expected to validate the City's technology asset inventory during transition.

**Question 23**: Is there a body camera system in place that we must maintain, or does the PD do that? Does the bodycam footage get uploaded as soon as the car pulls into the PD?

**Answer 23**: The Police Department operates a body-worn and in-car camera system. Routine administration of the camera system, camera hardware, evidentiary video, retention, and other law-enforcement-specific functions are not intended to become the responsibility of the managed IT provider under the Base Monthly Support scope.

The selected provider will, however, be expected to support the City-managed network, server, connectivity, and other underlying IT infrastructure upon which the system relies and to provide reasonable technical troubleshooting and vendor coordination when necessary.

The City is not providing detailed information regarding the system's video-transfer, upload, storage, or evidentiary workflow in a public addendum. Additional information necessary to support the underlying IT environment will be provided to the selected provider during transition, subject to appropriate security and confidentiality requirements.

**Question 24**: How many city employees use AI for their daily job functions, and do you know what kind of protection you have against AI cyber-attacks?

**Answer 24**: The City has not conducted a formal Citywide inventory or survey establishing the number of employees who use artificial intelligence tools as part of their daily job functions. Accordingly, the City does not have a verified employee count available for proposal purposes.

The City recognizes that artificial intelligence may be used by threat actors to enhance phishing, social engineering, credential attacks, malware, reconnaissance, and other cybersecurity threats. The City addresses these risks as part of its broader cybersecurity posture rather than through a separately defined “AI cyber-attack” program.

Proposers may describe their experience addressing emerging AI-enabled cybersecurity threats and any recommendations they believe would be appropriate for a municipal environment such as the City's.

**Question 25**: Which software would you most likely be looking into replacing in the near future, and what would you consider a good amount of replacement software recommendations, 2-3, 3-5 etc.?

**Answer 25**: The City has not identified a specific major software application that it currently intends to replace in the near term. As stated in Addendum 3, known near-term technology activities are primarily routine projects such as switch replacements, workstation replacements, and license renewals.

The City expects the selected provider to become familiar with the City's existing software and technology portfolio and recommend replacement, consolidation, modernization, or other changes where there is a demonstrated operational, cybersecurity, lifecycle, compatibility, or financial benefit. Any significant software replacement or migration would be evaluated and separately authorized by the City. The City has not established a required number of replacement recommendations. Recommendations should be driven by identified needs rather than a numerical quota. When recommending replacement of a material software system, the City would generally find it helpful for the provider to identify approximately two to three viable alternatives, where reasonably available, together with the provider's recommended option and the basis for that recommendation.

Recommendations should consider factors such as functionality, compatibility with the City's environment, cybersecurity, implementation requirements, lifecycle costs, recurring costs, support requirements, and operational impacts.

**Question 26**: Please confirm the anticipated contract award date and the expected period of performance commencement for this engagement. If a specific base period start date has been established or targeted by the Contracting Officer, provide that date along with any known constraints — such as fiscal year alignment, incumbent contract expiration, or required regulatory approvals — that may affect the award or activation timeline. If a start date has not yet been determined, describe the approval of milestones remaining before award can be executed.

**Answer 26**: The City has not established a specific contract award date. Proposals are due August 28, 2026, after which proposals will be reviewed in accordance with the evaluation process described in the RFP and prior addenda.

As described in Addendum 4, following staff review a Council-level committee will receive the proposals and determine a recommendation to the City Council. The RFP also reserves the City's right to request additional information, interview proposers, negotiate modifications, or take other actions determined to be in the City's best interest. Accordingly, the precise award date will depend upon completion of the evaluation, recommendation, approval, and contract-negotiation process.

The current term of the City's core managed IT support agreement is scheduled to end December 31, 2026. Accordingly, the City's objective is for the selected provider to be prepared to assume responsibility for the applicable core managed-services functions on or about January 1, 2027, subject to completion of the procurement, contract execution, and an orderly transition.

Transition and onboarding activities may need to begin prior to the operational commencement date. Proposers should describe the transition period they recommend and identify any lead time, dependencies, or City/incumbent-provider coordination necessary to achieve continuity of service.

Certain separately contracted technology services extend beyond the expiration of the City's core managed IT agreement. The transition plan will therefore need to account for those existing obligations and avoid unnecessary duplication of services or costs.
No separate fiscal-year alignment or regulatory approval requirement has been established in the RFP as a prerequisite to commencement. The contract will be subject to applicable City procurement requirements, required City approvals, availability and appropriation of funds for future fiscal periods, business-license requirements, applicable CJIS requirements, and other legal or contractual requirements relevant to the services performed.

**Question 27**: The RFP lists an asset portfolio assessment under Professional Services. Would it make more sense for proposers to scope that as a formal deliverable during transition (say first 90 to 120 days) with findings presented to leadership, or is that something the City sees as more of an ongoing function within the base monthly support?

**Answer 27**: The RFP distinguishes between routine asset inventory management and a formal asset portfolio assessment. As part of Base Monthly Support and transition, the selected provider will be expected to validate the City's existing technology asset inventory, identify active and inactive assets, correct material inventory gaps, and establish an accurate baseline for ongoing asset management.

The more comprehensive asset portfolio assessment identified under Professional Services is intended to go beyond inventory validation and may include analysis of utilization, lifecycle, redundancy, consolidation opportunities, right-sizing, replacement priorities, and other strategic recommendations.

The City has not mandated that the formal asset portfolio assessment occur within a specific timeframe. However, proposers may recommend performing it as an early Professional Services deliverable following transition—such as within the first 90 to 120 days—if they believe that timing would provide useful information to City leadership. Any formal asset portfolio assessment would be separately authorized and priced consistent with the Professional Services provisions of the RFP.

**Question 28**: On the Quarterly Operational Review and the 3-year technology roadmap, what format is the City expecting? A written document with year-by-year objectives and cost projections, or more of a presentation-style briefing?

**Answer 28**: The City has not prescribed a specific template for either deliverable and is open to proposers' recommended formats.

For the Quarterly Operational Review, the City anticipates an executive-level briefing supported by concise written or presentation materials addressing the areas identified in the RFP, including operational trends, recurring issues, infrastructure health, cybersecurity events, asset lifecycle concerns, and recommended actions. The emphasis should be on clear, decision-useful information rather than production of a lengthy formal report each quarter.

For a formal three-year technology roadmap, the City would expect a more comprehensive written deliverable suitable for use by executive leadership in technology, budget, and capital planning. At a minimum, the roadmap should identify major objectives and recommended initiatives by year, priorities, anticipated timing, dependencies, lifecycle considerations, and reasonable planning-level cost estimates or ranges where available.

The City would also expect the roadmap and its principal recommendations to be presented to City leadership in a briefing or presentation format. Proposers may describe the formats and methodologies they typically use for both quarterly reviews and multi-year technology roadmaps.

Respectfully,

Sean H. Kuester
Deputy City Administrator