TOWN OF TYRONE
ADDENDUM NO. 2
REQUEST FOR PROPOSALS
Managed Information Technology & Cybersecurity Services
RFP No. TH-2026-03

Issue Date: November 20, 2026

This addendum forms part of the Request for Proposals for Managed Information Technology & Cybersecurity Services. Respondents shall acknowledge receipt using the Addenda Acknowledgement form in Section 11.

The Town received numerous questions addressing overlapping subjects. Related questions have been consolidated and paraphrased for clarity. Respondents should review this entire addendum, as a response may address questions submitted by multiple firms. These responses apply to all prospective proposers.

Question No. 1

How must the prime perform core services, and what subcontracting is allowed?

Response:

The Town will accept complete proposals from a single U.S.-based prime contractor, including firms based outside Georgia that can meet all onsite and service-level requirements. The prime must use its own employees to provide day-to-day help desk support, routine and emergency onsite support, network and systems administration, Microsoft 365 administration, and day-to-day cybersecurity management and incident coordination.

The Town may approve subcontractors for discrete specialist services such as Drupal hosting or support, independent security assessments, specialized forensic response, or 24/7 SOC monitoring. If a third-party SOC is proposed, the prime must handle escalation, coordinate incident response, and communicate with the Town. The prime and all subcontractors must be based in the United States. See Q34 for offshore delivery.

Identify each proposed subcontractor, its assigned work, and any required access to Town systems or data. Identify the prime's staff responsible for core services. The prime remains responsible for all performance and service levels. Adding or replacing a subcontractor requires prior written Town approval.

Question No. 2

What experience and references must the prime provide?

Response:

Under Addendum No. 1, the prime must document its own local-government managed IT and prior GCIC/CJIS experience and submit three governmental or comparable references for work it performed. A proposer may include attributed qualifications, references, and project

experience for a disclosed specialist subcontractor. The Town will consider them only for the discrete services assigned to that subcontractor.

Question No. 3

Do participation or geographic preferences apply?

Response:

The Town does not apply a small-business, veteran-owned business, or HUBZone preference or require participation reporting for these categories under this solicitation.

Question No. 4

What GCIC/CJIS qualifications are required and when?

Response:

Proposers should already have GCIC experience and applicable certifications and clearances for proposed personnel. Describe the prime's relevant experience and identify qualified staff and their current qualifications in the proposal. Access is subject to verification and any applicable Town-specific approvals.

Question No. 5

How is GCIC/CJIS onboarding coordinated?

Response:

The GBI/GCIC vetted vendor program coordinates fingerprinting, training, and vendor onboarding. After vetting, the provider signs a vendor agreement with the agency and provides its scope of services. Personnel must meet applicable GCIC/CJIS requirements before accessing covered Police or Municipal Court systems. The Town's Terminal Agency Coordinator is April Spradlin. Consult the GCIC Council Rules and GCIC Operating and Policy Manual at https://gcicweb.gbi.state.ga.us/publications.

The Town will not consider vendors that do not have existing personnel with GCIC/CJIS experience and applicable certifications and clearances.

Question No. 6

What Police and Municipal Court systems are within scope?

Response:

The managed IT scope includes Police and Municipal Court endpoints, patrol laptops, server and file services, access administration, endpoint security, and coordination with application vendors. Motorola/WatchGuard supports body and in-car camera hardware and the Evidence Library application. Courtware and Tyler Incode are vendor-hosted. The GCIC terminal and state connectivity are separately supported. Personnel accessing applicable systems must satisfy GCIC/CJIS requirements and provide proof of prior experience. The Town will not consider vendors that do not have existing personnel with GCIC/CJIS experience and applicable certifications and clearances.

Question No. 7

What sites and network equipment are in scope?

Response:

Town Hall, Police, and Municipal Court share the building at 950 Senoia Road. The Library and Recreation Office are housed in separate facilities and each have a separate network rack. The main site uses WOW internet with cellular failover. VC3's inventory lists one Sophos firewall, three Cisco Meraki switches (MS125-48FP, MS125-48LP and MS250-48LP), three UniFi access points on record, and one Cradlepoint AER2200. VC3 does not maintain a complete printer inventory.

Question No. 8

What servers are in the current inventory?

Response:

VC3's inventory identifies three physical servers and two virtual servers. Police has a 2015 Dell PowerEdge T420 with expired warranty, running Windows Server 2012 R2 and hosting one Windows Server 2012 R2 virtual server. These support evidence and Police/Court directory and file services. Police also has a 2023 Dell PowerEdge T550 running Windows Server 2022 with warranty listed through October 2028. Administration has a 2020 Dell PowerEdge T440 running Windows Server 2019 with expired warranty, plus one Windows Server 2019 virtual server used for a legacy application share.

Administration is open to eliminating its physical server if file/document storage and management needs can be facilitated by M365 (OneDrive/SharePoint).

Question No. 9

What Microsoft 365 licenses does the Town maintain and how should they be priced?

Response:

The Town uses a commercial Microsoft 365 tenant and purchases its licenses directly from Microsoft. Its inventory lists 40 Exchange Online (Plan 1), four Business Basic, 25 Business Standard, and two Planner and Project Plan 3 licenses. Price administration of these accounts. Exclude the Town's direct subscription costs.

Question No. 10

What security and management tools are in place and which will transfer?

Response:

The incumbent environment includes remote monitoring and management, Splashtop remote access, CrowdStrike endpoint protection and monitored server backups. Current VC3 services do not include 24/7 SOC monitoring, email or DNS/web filtering, dark-web monitoring, security awareness training, Microsoft 365 backup or an enforced MFA service. Propose and price the capabilities required by the RFP. The incumbent can export backup data, while the existing backup licenses and backup jobs do not transfer directly.

Question No. 11

What backup environment and recovery requirements should proposers use?

Response:

VC3 currently backs up four server workloads nightly using MSP360, with local NAS and offsite Wasabi cloud copies. Current retention is approximately 7–30 days onsite and 91 days offsite. The historical local backup footprint was approximately 9–19 TB in October 2025 and included substantial video data. Current offsite volume remains unverified. Restores are performed on request and VC3 reports no documented RTO or RPO. VC3's backup service excludes endpoints, Microsoft 365, vendor-hosted applications and camera recorders. Describe proposed backup coverage, retention, restoration testing and recovery targets under Section 4.7.

Question No. 12

What Vonage services should proposers price?

Response:

Price administration of the existing Town-owned, directly billed Vonage Business account, including account and extension administration, call groups, company recordings and support for the 36 Yealink SIP-T21P desk phones identified in the RFP. VC3 does not administer Vonage. The November 2026 invoice lists 29 unlimited extensions, one virtual extension, four local numbers, two fax numbers, seven call groups and two Vonage for Office 365 licenses. These are historical invoice counts. The Town intends to retain Vonage and is not interested in quotes for new phone services.

Question No. 13

Should proposers price security camera or NVR management?

Response:

The Town intends to exclude security camera and Network Video Recorder (NVR) administration from this procurement.

Question No. 14

What website platform and hosting environment should proposers assume?

Response:

VC3 hosts and maintains the Town's Drupal 10 website on Microsoft Azure virtual machines. VC3 reports approximately 3.7 GB of website files and a 689 MB database, no custom modules and Google Analytics as the identified third-party integration. Town staff estimate approximately 12 content editors.

Question No. 15

What will be available for the website transfer?

Response:

For pricing purposes, assume VC3 will provide an export of page content and a ZIP archive of all user-uploaded documents and images. VC3 has advised that its site code and raw database

will be unavailable. Section 4.9 is revised to require a rebuild and content migration on a supported platform. Preserve the current site's main navigation and public functions as closely as practical. Migrate the content and files, preserve or redirect existing public URLs, test the site, and coordinate a Town-approved cutover. A separate hosting provider is acceptable. Schedule any planned downtime outside business hours. The Town intends to keep the current site live through acceptance and cutover under a separate transitional hosting arrangement. See Question 23 for pricing.

Question No. 16

What historical support volumes are available?

Response:

From November 2025 through October 2026, VC3 recorded 370 tickets, an average of about 31 per month. Of these, 108 were staff-initiated, averaging nine per month, and 262 were automated alerts. Priority totals were 57 critical, 132 high and 181 medium, with nearly all critical and high tickets attributed to automated alerts. There were 132 after-hours entries, five initiated by staff, and four routed to the after-hours team. Police/Court accounted for 120 tickets, including 35 staff-initiated. Two tickets were flagged for onsite support, with no confirmed visits in the reporting period. Workstation deployments were completed remotely. A printer dispatch occurred November 12, 2026, outside the reporting period.

Question No. 17

What onsite support model and arrival times does the Town expect?

Response:

The Town prefers a remote-first model. The prime's own employees must provide routine and emergency onsite support when needed, as required by Addendum No. 1.

Question No. 18

What initial response times and support hours apply?

Response:

Section 5 specifies a 30-minute initial response for critical incidents, 24/7. It lists a one-hour initial response for high-priority incidents.

Question No. 19

What is the incumbent arrangement and anticipated transition?

Response:

VC3 provides the incumbent service under month-to-month agreements terminable on 30 days' written notice. No equipment leases or financing through VC3 were reported. Key scope differences include expanded security services, routine onsite support and workstation deployments, Vonage administration and Microsoft 365 backup. VC3 states its standard offboarding typically takes at least 45 days, with timing confirmed upon notice. It can provide IT Glue documentation, asset and configuration records, secure administrative handoff, Meraki dashboard access, available vendor contacts and a copy of backup data on external media. Direct transfer of backup software licenses and jobs is unavailable.

The Town intends to arrange temporary hosting with VC3 under a separate work order to keep the current website live during any potential rebuild and through the Town-approved cutover. This website arrangement is separate from the managed IT offboarding schedule. See Question 15 for the website handoff.

Question No. 20

What assumptions apply to optional modernization estimates?

Response:

The Town seeks the provider's recommendation on an appropriate Microsoft 365 government environment and server replacement specifications. The Town has not selected a government tenant. Use the available server and backup inventory for preliminary estimates and identify your assumptions.

Question No. 21

What insurance limits and documentation will be required?

Response:

Proposed minimum insurance limits:
• Commercial general liability: $1,000,000 per occurrence and $2,000,000 aggregate.
• Automobile liability: $1,000,000 combined single limit per accident. Hired and non-owned auto coverage may satisfy this requirement if the firm owns no vehicles and the coverage applies to its work for the Town.
• Workers' compensation: statutory limits, as applicable.
• Employers' liability: $1,000,000 each accident, $1,000,000 disease per employee, and $1,000,000 disease policy limit.
• Technology errors and omissions: $1,000,000 per claim and in the aggregate.
• Cyber liability: $2,000,000 per claim and in the aggregate.

A combined technology E&O and cyber policy may satisfy both requirements with a shared limit of at least $2,000,000 per claim and in the aggregate, provided both coverages apply to the services in the RFP. For any approved specialist subcontractor, the prime must show that its policies cover their work or that they carry appropriate coverage of their own, particularly if they access Town systems or data.

Question No. 22

Will the Town provide its budget, historical spending, or a draft agreement?

Response:

The Town will not provide a target budget. Submit your best pricing for the required services.

The Town will not provide a draft agreement. As part of the proposal submission under Section

7, each proposer must include its own proposed contract or services agreement covering the services offered.

Question No. 23

What recurring pricing and equipment growth assumptions should proposers use?

Response:

The Town anticipates approximately five routine device replacements per year and roughly one additional device every 18–24 months. No change in facility count is anticipated. The Town prefers per-user pricing and requires a full-scope proposal. Use the Section 8 schedule.

Supplement the Section 8 pricing schedule with a separately identified one-time price for the website rebuild, content migration, testing, and cutover. Separately identify recurring website hosting and support. Exclude the Town's separate VC3 transitional hosting charges from the proposal. State the assumptions behind the website pricing.

Question No. 24

What counts toward the page limit and how should forms be submitted?

Response:

Section 7 excludes pricing, required forms, resumes, and supplemental technical documentation specifically requested by the Town from the 20-page limit.

Question No. 25

What are the deadlines and submission instructions?

Response:

Written questions were due November 16, 2026, at noon Eastern Time. Proposals are due December 4, 2026, at 2 p.m. Eastern Time. Follow the delivery and addendum acknowledgment instructions in the RFP.

Question No. 26

Will the Town offer a pre-proposal site visit or controlled technical discovery?

Response:

We are not offering pre-proposal site visits.

Question No. 27

What endpoint inventory should proposers use?

Response:

VC3's November 17 management inventory lists 49 Windows endpoints. Of these, 26 are Police/Court devices, including 13 patrol laptops, and 23 are assigned to Town Hall, Library and Recreation. The inventory contains 41 Windows 11 devices and eight Windows 10 devices. VC3 reports approximately nine devices in warranty, 36 with expired warranties and four with

unknown status. Common makes include Dell and Microsoft Surface, with one HP. Elected officials use basic Microsoft accounts and have no Town-issued devices according to staff.

Question No. 28

Which patrol devices and specialized Police technologies are in scope?

Response:

Patrol laptops are within the managed endpoint inventory. VC3 lists 13, including 12 Dell Latitude 5430 Rugged laptops and one Dell Vostro. The managed service covers device and authorized access support. Specialized hardware and applications such as in-car cameras, body-worn cameras and the Evidence Library application remain supported by their respective vendors. The managed provider coordinates authorized access and supports the underlying Town systems.

Question No. 29

Are hardware refreshes or other technology changes planned?

Response:

We do not anticipate any material changes, expansions, or new initiatives at this time.

Question No. 30

Does the scope include additional support for events and public-facing technology?

Response:

The RFP does not include additional event, temporary communications, or public-facing technology support of the kind described in the bidder questions.

Question No. 31

What Town applications and development work are in scope?

Response:

Proposals should only cover the scope listed in the RFP.

Question No. 32

Is additional vendor registration or licensing required?

Response:

No separate vendor registration, portal enrollment, or additional submission step is required to participate. Proposers must follow the submission instructions in Section 7 and include the required forms.

The Town does not require proof of Georgia Secretary of State registration or a Town occupational tax certificate (business license) with the proposal. The selected proposer is responsible for obtaining any registration, certificate of authority, or occupational tax certificate that applies to its business before beginning activities for which it is required.

Georgia registration depends on the entity type and its activities in Georgia. The Town's occupational tax certificate applies to businesses located in Tyrone. Submitting a proposal does not, by itself, require either credential.

Question No. 33

What E-Verify information must be submitted?

Response:

Submit the applicable Section 11 affidavit with the proposal. The form requests the proposer's E-Verify user identification number and authorization date where applicable.

Question No. 34

May work be performed or Town systems accessed from outside the United States?

Response:

Addendum No. 1 requires the prime and all subcontractors to be based in the United States and to perform services and access Town systems and data from within the United States. This includes subcontracted website work.

Question No. 35

Is a separate body-camera storage deployment required?

Response:

The Town currently stores body-camera footage on Police server infrastructure. Proposers should distinguish support for the underlying infrastructure from manufacturer support of the evidence application and equipment.

Question No. 36

What evidence of provider cybersecurity is acceptable?

Response:

The Town does not require a SOC 2 report for award. Under Section 4.6, proposers may submit relevant evidence of their security program, including a SOC 2 Type II report, ISO/IEC 27001 certification, an independent security assessment, or CMMC Level 1 status with supporting policies and incident-response procedures. The Town will evaluate the evidence based on its scope and relevance to the proposed services and may request supporting documentation. Applicable GCIC/CJIS requirements remain in effect.

Question No. 37

How will the Town award the 35 cost points?

Response:

Section 9 assigns 35 points to cost. Lower evaluated overall cost will receive a higher score.

Question No. 38

What monitoring, scanning, and training should base pricing include?

Response:

VC3 currently provides CrowdStrike endpoint protection and remote monitoring and management. Its current service does not include 24/7 security operations center (SOC) monitoring, email filtering, DNS/web filtering, dark-web monitoring, or security awareness training. The Town does not currently have a phishing simulation tool in place and requests this capability in this RFP. The Town handles CJIS awareness training and its agency compliance activities. The provider must satisfy applicable GCIC/CJIS requirements for its own access and work.

Question No. 39

What security policies, audits, and insurer controls apply?

Response:

The provider must comply with applicable GCIC/CJIS policies and the GBI vetted vendor requirements. Staff identify a current vendor agreement and a network topology diagram as GCIC audit support items.

Question No. 40

Where must Town data be stored and processed?

Response:

Addendum No. 1 requires the prime contractor and all subcontractors to perform services and access Town systems and data from within the United States. That requirement also applies to the storage of CJI data.

For non-CJI data, identify the countries where each proposed platform will store or process Town data, including ticketing, remote monitoring and management, website hosting, backups, disaster recovery copies, and logs. Disclose any storage or processing outside the United States and identify the third-party providers involved. Any proposed storage or processing outside the United States is subject to the Town’s prior written approval. Systems that handle CJI must meet applicable GCIC/CJIS requirements.

Question No. 41

How should proposers handle trade-secret claims?

Response:

Proposals and all associated submittals are subject to the Georgia Open Records Act as stated in Section 7.