TOWN OF TYRONE
950 Senoia Road
Tyrone, Georgia 30290
Attn: Brandon Perkins, Town Manager
Email: brandon.perkins@tyronega.gov

SUBJECT: RFP # TH-2026-03 Request for Proposals for Managed Information Technology & Cybersecurity Services

DATE OF RFP RELEASE: November 2, 2026

Section 1 – Invitation

The Town of Tyrone, Georgia ("Town") is soliciting sealed proposals from qualified Managed Service Providers ("MSPs") to provide comprehensive information technology management, end-user support, cybersecurity, website management, Microsoft 365 administration, backup and recovery, and strategic technology services.

The Town does not maintain an internal information technology department. The selected provider will serve as the Town's primary technology partner and will be expected to provide reliable day-to-day support while proactively managing the Town's technology environment, cybersecurity posture, business continuity, and long-term technology needs.

The Town seeks a provider with demonstrated experience supporting local government environments, including law enforcement and systems subject to GCIC/CJIS requirements.

The Town reserves the right to reject any or all proposals, waive minor irregularities, request clarification, negotiate with one or more proposers, cancel or reissue this RFP, and award a contract determined to be in the best interest of the Town.

Section 2 – Procurement Schedule

Event	Date
RFP Issued	November 2, 2026
Deadline for Written Questions	November 16, 2026 @ 12pm
Responses/Addenda Issued	November 20, 2026 @ 4pm
Proposal Due / Opening	December 4, 2026 @ 2pm
Proposal Evaluation	December 11, 2026 @ 10am
Council Award	January 21, 2027 @ 7pm
Service Commencement	TBD

Dates may be modified by written addendum.

Procurement Contact

Brandon Perkins, Town Manager
Town of Tyrone
950 Senoia Road
Tyrone, Georgia 30290
brandon.perkins@tyronega.gov

All questions must be submitted in writing. Only written addenda issued by the Town shall modify this RFP.

Section 3 – Current Technology Environment

The following represents the Town's best current estimate and is provided for proposal and pricing purposes. Quantities are approximate and may change:

Department	Laptops	Desktops	Tablets	Users	Physical Servers
Police	23	2	0	17	2
Public Works	4	1	5	4	0
Municipal Court	5	0	0	3	0*
Parks & Recreation	2	0	0	2	0
Community Development	2	0	1	2	0
Library (Town-Owned)	1	5	0	6	0*
Administration/Finance	6	0	0	6	0
Known Totals	43	8	6	40	2

* Municipal Court utilizes systems associated with the Police Department environment. Public-access/circulation technology and related systems at the Library are managed through the regional library system and are not included in the Town-owned inventory.

The inventory is provided for informational purposes and is not warranted to be exhaustive. Proposers should account for reasonable fluctuations in users and devices during the contract term. The successful provider shall perform an initial technology assessment and establish and maintain a comprehensive inventory of Town IT assets, systems, network infrastructure, software, licensing, administrative accounts, and related documentation.

The Town currently utilizes Microsoft 365 and associated identity, security, archiving, and data-protection services.

Section 4 – Scope Of Services

The selected provider shall furnish the personnel, expertise, systems, tools, and services necessary to manage and support the Town's technology environment. Equivalent or superior technologies may be proposed. The Town is interested in required capabilities and outcomes rather than a particular proprietary technology stack.

4.1 - Help Desk and End-User Support

- Remote help desk support for Town personnel.
- 24x7x365 response for critical technology and cybersecurity incidents.
- Routine onsite support when remote support is impractical or unsuccessful.
- Computer, tablet, printer, peripheral, and approved software support.
- User onboarding, modification, and termination.
- Hardware and software troubleshooting.
- Coordination with third-party technology vendors.

Routine onsite support necessary to maintain the existing Town environment shall be included in the fixed managed services fee.

Routine new and replacement workstation setup and deployment shall include device configuration, standard software and security installation, user setup, data/profile transfer where applicable, and connection to Town networks and printers. Proposers shall disclose any per-device deployment fee and distinguish routine deployments from separately authorized major projects.

4.2 - Monitoring and Infrastructure Management

- Proactive monitoring, administration, maintenance, and support of applicable servers, workstations, laptops, network equipment, firewalls, wireless infrastructure, operating systems, and other Town-managed technology infrastructure.
- Patch management, system health and performance monitoring, and proactive identification and remediation of technology issues.
- The provider shall support the network connectivity, switching, access controls, and cybersecurity of Town-connected security camera systems. Proposers shall state whether camera/NVR configuration, firmware maintenance, recording/storage administration, and camera troubleshooting are included, excluded, or available as an optional separately priced service. The Town will confirm camera-system equipment and ownership during discovery.
- The Town also operates network equipment in separate facilities serving the Library and Parks & Recreation offices. Each has a dedicated network rack room rather than a conventional server room. Proposers shall include routine monitoring, administration, troubleshooting, and necessary onsite support for Town-managed equipment at these locations.

4.3 - Microsoft 365 and Identity Management

- Administration and support of Microsoft 365 licensing, Exchange/email, Entra ID, multifactor authentication, archiving, security services, and cloud data protection/backup.
- Licensing management and recommendations to improve security, functionality, or cost efficiency.

4.4 – Vonage Business VOIP Phone Management

- Administration and support of the Town's Vonage Business enterprise license. This includes end user account management, extension management, call groups, and company recordings.
- Support of physical hardware devices currently including 36 Yealink SIP-T21P VOIP desk phones.

4.5 - Cybersecurity

- Managed Endpoint Detection and Response (EDR).
- 24x7x365 security monitoring/Security Operations Center capability.
- Email security and spam filtering.
- Web/content protection.
- Multifactor authentication.
- Security awareness training.
- Credential/dark-web monitoring.
- Vulnerability identification and remediation.
- Security incident detection and response.
- Ongoing cybersecurity recommendations.

The provider shall promptly notify designated Town personnel of significant cybersecurity incidents and assist with containment, investigation, recovery, documentation, and coordination with appropriate third parties.

4.6 - Provider Security Requirements

- Require multifactor authentication for privileged and remote administrative access.
- Apply least-privilege practices and appropriately restrict administrative credentials.
- Maintain appropriate endpoint protection and security monitoring for systems used to access the Town environment.
- Maintain documented cybersecurity incident-response procedures.
- Promptly notify the Town of any actual or suspected security incident that may affect Town systems, accounts, credentials, or data.
- Maintain appropriate controls over employees, subcontractors, and other personnel with access to Town systems.
- Comply with applicable GCIC/CJIS requirements when accessing applicable Police or Court systems.
- Maintain cyber liability insurance.
- Cooperate with the Town, law enforcement, insurers, forensic investigators, and other authorized parties following a cybersecurity incident.
- Disclose subcontractors or third-party service providers that will have administrative access to Town systems or sensitive Town information.

Proposers shall identify relevant cybersecurity certifications, independent security assessments, SOC reports, penetration testing, or other measures used to evaluate the security of the proposer's own environment. The Town may request supporting documentation during evaluation.

4.7 - Backup, Recovery and Business Continuity

- Monitor backup success and failures.
- Maintain appropriate retention.
- Periodically test restoration capabilities.
- Assist with restoration following data loss or system failure.
- Maintain documented recovery procedures for critical Town systems.

The proposer shall describe its proposed backup architecture, retention practices, restoration testing, and disaster-recovery capabilities.

4.8 - Police, Court and GCIC/CJIS Support

The provider must be capable of supporting the Town's Police Department and Municipal Court technology environments. Personnel requiring access to Criminal Justice Information (CJI) or applicable systems must satisfy all applicable GCIC/CJIS security, background, training, authentication, and access-control requirements. Proposers shall describe their experience supporting Georgia law enforcement, courts, or other criminal justice agencies and their ability to provide appropriately qualified personnel.

4.9 - Website Management and Support

The Town's website – www.tyronega.gov – was developed on the Drupal CMS and is maintained and hosted by our current IT Services provider (VC3). If a new vendor is selected, the website will need to be transferred to a new host with minimal downtime. Proposers who cannot facilitate this transfer must make that clear in their proposal. The Town is not currently interested in a new design, so maintaining the current site and securing its data is vital.

The following are required on-going expectations for website support:

- Website hosting administration and coordination.
- Content management system administration.
- User account and access management.
- Software, plugin, theme, and security updates.
- Website security monitoring and remediation.
- SSL certificate and domain/DNS management or coordination.
- Website backup and recovery.
- Troubleshooting website functionality and availability.
- Technical support for Town staff responsible for website content.
- Coordination with third-party website vendors or service providers.
- Assistance implementing website technology improvements and integrations.
- Assistance with coming ADA compliance requirements for government websites.

The provider shall maintain appropriate administrative documentation and ensure that the Town retains ownership and administrative control of its domain, website accounts, website content, credentials, and associated data. The provider shall provide reasonable technical assistance with website accessibility and implementation of accessibility-related technology changes directed by the Town; however, the provider shall not be considered the Town's legal or regulatory compliance advisor.

4.10 - Strategic Technology Services

- Technology planning.
- Equipment lifecycle and replacement planning.
- Budget planning.
- Cybersecurity recommendations.

- Hardware and software procurement assistance.
- Technology policy guidance.
- Third-party vendor coordination.
- Periodic review of the Town's technology environment.

The provider shall proactively identify significant risks, deficiencies, unnecessary expenditures, and opportunities for improvement.

4.11 - Optional Technology Modernization Projects

The Town requests separate, nonbinding preliminary estimates for (1) assessment and replacement or migration of aging physical servers, including cloud-hosted alternatives, and (2) migration of its Microsoft 365 commercial tenant to an appropriate government tenant. For each, proposers shall identify assumptions, estimated one-time costs, anticipated recurring cost changes, key dependencies, expected downtime, and the discovery needed to develop a firm proposal. These projects are optional, are not part of the base managed services fee, and will require separate Town approval.

Section 5 – Service Level Expectations

The proposer shall provide its standard Service Level Agreement and identify any exceptions to the following minimum initial-response expectations:

Priority	Example	Maximum Initial Response
Critical	Town-wide outage, critical server/network failure, active cybersecurity incident, public-safety system outage	30 minutes, 24x7
High	Significant operational impact, multiple users, critical Town function	1 hour
Normal	Individual user issue or routine service request	4 business hours

The provider shall maintain a ticketing system capable of documenting service requests, response and resolution activity, escalation, and recurring issues. Proposers shall describe escalation procedures and proposed resolution/service-restoration targets.

Section 6 – Transition And Documentation

- Conduct an initial discovery and technology assessment.
- Establish a complete technology and asset inventory.
- Review network, security, and backup configurations.
- Obtain and document necessary administrative credentials.
- Identify significant technology or cybersecurity risks.
- Provide the Town with an initial findings and recommendations report.

All Town data, accounts, administrative credentials, configurations, documentation, inventories, licensing records, backup information, and other technology records shall remain the property of the Town. The Town shall maintain independent administrative access to critical Town systems, and the provider shall not maintain exclusive control of credentials necessary to operate the Town's environment.

Where reasonably practicable, Town systems, domains, cloud services, software subscriptions, and administrative accounts shall be established in the Town's name rather than the provider's name. The provider shall not structure the Town's environment in a manner that unnecessarily restricts transition to another service provider.

Upon expiration or termination, the provider shall reasonably cooperate with the Town and any successor provider and promptly transfer Town information, credentials, configurations, documentation, and other records necessary for continuity of operations.

Section 7 – Proposal Requirements

The proposal (bid) must be submitted upon a flash drive with a pdf copy of the proposal (bid) plus one hard copy of the proposal and all supplemental documentation must be enclosed in a sealed envelope clearly titled, **RFP # TH-2026-03 Request for Proposals for Managed Information Technology & Cybersecurity Services** and delivered to the address below.

All proposals must clearly bear the Respondent's name and address:

Town of Tyrone
Attn: Brandon Perkins, Town Manager
950 Senoia Road
Tyrone, Georgia 30290
brandon.perkins@tyronega.gov

Hand delivered copies may be delivered to the above address ONLY between the hours of 8:00 a.m. and 5:00 p.m. ET, Monday through Friday, excluding holidays observed by the Town of Tyrone.

The proposal must be signed by a company officer or agent who is legally authorized to enter into a contractual relationship in the name of the Respondent.

Ownership of all data, materials, and documentation prepared for and submitted in response to this RFP shall belong exclusively to the Town of Tyrone and will be considered a public record and subject to public inspection in accordance with the Georgia Open Record Act, O.C.G.A. § 50-18-70 et. seq. unless otherwise provided by law.

All expenses involved with the preparation and submission of the RFP to the Town of Tyrone, or any work performed in connection therewith is the responsibility of the Respondents.

The Town of Tyrone reserves the right to extend the deadline for submission of proposals, call for new proposals, and to waive any irregularities or informalities in any proposal or in the submittal procedure. Failure to comply with the requirements set forth in this RFP may result in disqualification. Submitted proposals may be withdrawn at any time prior to the submission time specified in this RFP, provided notification is received in writing before the submittal deadline. Proposals cannot be changed or withdrawn after the submittal deadline. No handwritten notations or corrections will be allowed.

The Town reserves the right to reject any or all proposals and to waive any minor informalities or irregularities contained in any proposal. Acceptance of any proposal submitted pursuant to this RFP shall not constitute any implied intent to enter into a contract. The contract award, if any, will be made to the Respondent who, in the Town's sole discretion, is best able to perform the required services in a manner most beneficial to the Town.

Proposals should be concise and should contain the following:

1. Company Overview and Qualifications.
2. Municipal/Public-Sector Experience, including Georgia local government and public-safety experience. Include three (3) governmental or comparable references.
3. Proposed Service Model and Technical Approach.
4. Staffing and Support Model, including help desk, onsite support, escalation, and after-hours response.
5. Cybersecurity Approach.
6. GCIC/CJIS Capabilities.
7. Backup and Disaster Recovery Approach.
8. Website Management Approach.
9. Transition/Implementation Plan.
10. Completed Pricing Schedule.
11. Exceptions to any RFP requirement or proposed contract condition.

Proposals should not exceed 20 pages, excluding pricing, required forms, resumes, and supplemental technical documentation specifically requested by the Town. Marketing materials not directly responsive to this RFP are discouraged.

Proposals shall also describe workstation deployment practices; support for the Town's separate Library and Recreation network facilities; security camera system capabilities and exclusions; and the approach, assumptions, and preliminary pricing for the optional projects identified in Section 4.11.

Section 8 – Pricing

The Town prefers a predictable fixed-cost service model. Proposers shall complete the following pricing schedule:

Pricing Component	Proposed Cost
Fixed Monthly Managed Services Fee	$_____
Required Software/Security/Backup Licensing	$_____ / month
Microsoft 365 Licensing	$_____ / month
Other Recurring Charges	$_____ / month
TOTAL MONTHLY RECURRING COST	$_____
One-Time Transition/Implementation	$_____
Project/Engineering Rate, if applicable	$_____ / hour
After-Hours Non-Emergency Project Rate, if applicable	$_____ / hour
New/Replacement Workstation Deployment Fee (if any), per device	$_____
Optional Server Replacement / Cloud Migration – Preliminary One-Time Estimate	$_____
Optional Microsoft 365 Government Tenant Migration – Preliminary One-Time Estimate	$_____
Optional Camera/NVR System Management – Monthly Cost (if not included)	$_____

The fixed monthly managed services fee shall include all routine labor necessary to perform the Scope of Services, including help desk, remote support, routine onsite support, monitoring, administration, maintenance, cybersecurity management, Microsoft 365 administration, backup administration, website management and support, vendor coordination, documentation, and strategic IT support.

Routine setup and deployment of replacement or additional Town workstations, including operating system configuration, standard applications, security tools, user profiles, and connection to existing systems, shall be included in the fixed monthly fee unless a separate per-device deployment charge is expressly identified in the pricing schedule. Hardware, software licenses, and major migrations may be priced separately.

Proposers shall separately identify all required software, licenses, subscriptions, security products, backup services, cloud services, or other recurring expenses not included in the fixed monthly fee. Any Scope of Services item resulting in an additional charge must be specifically identified. Charges not disclosed in the proposal may not be billed without prior written authorization from the Town.

Routine activities associated with maintaining, supporting, securing, and administering the Town's existing technology environment shall not be classified as separately billable projects.

Optional projects identified in this RFP shall be priced separately and shall not be included in the evaluated total monthly recurring cost. No optional project may proceed without separate written authorization from the Town.

Section 9 – Evaluation

The Town intends to make a best-value selection based upon the following criteria:

Criterion	Points
Cost	35
Technical Approach & Proposed Services	20
Qualifications & Municipal/Public-Safety Experience	15
Cybersecurity & GCIC/CJIS Capabilities	15
Service Model, Staffing & Responsiveness	10
References & Transition Plan	5
TOTAL	100

The Town may request clarification, conduct interviews, request demonstrations, or negotiate with one or more proposers before making a recommendation for award. Final award is subject to approval by the Mayor and Council.

Section 10 – Contract Requirements

The Town anticipates an initial two-year contract, with an optional one-year renewal at the sole option of the Town. The resulting agreement shall address, at minimum:

- Scope and service levels.
- Pricing and authorized additional charges.
- Confidentiality and data security.
- Protection of personally identifiable information and CJI.
- Cybersecurity incident notification and cooperation.
- Ownership and return of Town data and documentation.
- Transition assistance.
- Insurance.
- Compliance with applicable laws.
- E-Verify requirements.
- Termination provisions.

The Town anticipates requiring Commercial General Liability, Automobile Liability, Workers' Compensation, Professional/Technology Errors & Omissions, and Cyber Liability insurance. Final limits will be established in the contract documents.

The contract will be subject to review by the Town Attorney and approval by the Mayor and Council.

Section 11 – Required Forms

The following forms must be completed and submitted with the proposal.

EXECUTION OF PROPOSAL

Re: Town of Tyrone RFP # TH-2026-03 – Managed Information Technology & Cybersecurity Services

The Respondent certifies by signing below that:

☐ The proposal is signed by an individual authorized to bind the firm.

☐ The Respondent has reviewed the RFP and issued addenda and identifies any exceptions in its proposal.

☐ The Respondent is capable of performing the proposed services and certifies that its proposal meets the RFP requirements except as expressly disclosed.

☐ The proposal was prepared independently, fairly, and without collusion or fraud.

☐ The proposal shall remain valid for one hundred and twenty (120) days following the proposal due date.

The undersigned offers to enter into an agreement with the Town, if selected, subject to mutually agreed contract terms and approval by the Town. Georgia law shall govern the resulting contract.

Printed Name of Respondent Company

Address

Phone Email

EXECUTION OF PROPOSAL

Re: Town of Tyrone RFP # TH-2026-03 – Managed Information Technology & Cybersecurity Services

---

Authorized Signature Date

Printed Name & Title

Subscribed and sworn to before me this _____ day of _____, 20____.

Notary Public: _____

My Commission Expires: _____

(Notary seal)

ADDENDA ACKNOWLEDGEMENT

Re: Town of Tyrone RFP # TH-2026-03 – Managed Information Technology & Cybersecurity Services

The Respondent has examined the Request for Proposals and acknowledges receipt of the following addenda, if any:

Addendum No.	Date Received
_____	_____
_____	_____
_____	_____
_____	_____

If no addenda were issued, write "None" above.

Respondents must acknowledge any issued addenda. Proposals which fail to acknowledge the Respondent's receipt of any addendum will result in the rejection of the offer if the addendum contained information which substantively changes the Owner's requirements.

Authorized Signature Date

Printed Name & Title

GEORGIA SECURITY AND IMMIGRATION COMPLIANCE ACT AFFIDAVIT

Re: Town of Tyrone RFP # TH-2026-03 – Managed Information Technology & Cybersecurity Services

Name of Contracting Entity: _____

Contract No. and Name: _____

Contract Date: _____

By executing this affidavit, the undersigned person or entity verifies its compliance with O.C.G.A. § 13-10-91, affirming that the individual, firm, or corporation contracting with the Town of Tyrone has registered with, is authorized to participate in, and is participating in the federal work authorization program commonly known as E-Verify*, in accordance with applicable provisions and deadlines established in O.C.G.A. § 13-10-91.

The undersigned further agrees to continue using the federal work authorization program throughout the contract period and to contract for the physical performance of services only with subcontractors who provide affidavits containing the information required by O.C.G.A. § 13-10-91(b). The undersigned shall maintain required compliance records and provide copies of subcontractor verification to the Town when such subcontractors are retained.

_____ _____

EEV/E-Verify User Identification Number Date of Authorization

_____ _____

Authorized Officer or Agent Signature Date

_____

Title of Authorized Officer or Agent

_____

Printed Name of Authorized Officer or Agent

SUBSCRIBED AND SWORN BEFORE ME ON THIS _____ DAY OF _____, 20____

Notary Public: _____ (Notary Seal)

My Commission Expires: _____

*The federal work authorization program includes any successor program operated by the U.S. Department of Homeland Security.

PRICING CERTIFICATION

Re: Town of Tyrone RFP # TH-2026-03 – Managed Information Technology & Cybersecurity Services

The Respondent certifies that the pricing schedule in Section 8 is complete and identifies all recurring charges required to provide the proposed solution. All assumptions, exclusions, additional charges, and pricing exceptions are disclosed in the proposal.

Authorized Signature Date

Printed Name and Title