Network Support Services
RFP-RH-25-061
Proposals Opened: Wednesday,
November 19, 2025 @ 3:00 p.m.

NAME ADDRESS	ATT	Global Solutions Group 31681 Dequindre Road Madison Heights, MI 48071	IT Solutions Group 28175 Haggerty Road Novi, MI 48377	Maestro Technologies, Inc. 1 West State Street, 3rd Floor Trenton, NJ 08608	Recovery Point Systems, Inc. 75 West Watkins Mill Rd. Gaithersburg, MD 20878
Is the Vendor a Certified HPE Enterprise Partner or higher?		Infosys Public Services is HPE partnership. GSG promises Certified HPE Enterprise Partner delivery" for ICMS and DRMS via teaming with Infosys.	Yes	Yes. They supplied an HPE Certified Partner Number.	Recovery Point is a Tier II Enterprise Solution Partner.
Company Structure / Size; How many employees does company employ?		164 Employees. The company is organized into 3 primary services under the executive leadership: Document Management, IT Services, and Cybersecurity. Org chart provided.	10 full time, 8 part time employees	They have 218 personnel globally; 108 in the US, 98 in India, 12 in the UK. The dedicated team for the City project will work primarily from their headquarters in Trenton NJ. They included a chart on page 7 of their proposal.	They have over 100 employees
Principal Contact Person		Lisa Salvador, contact information provided	Greg Williams, contact information provided	Irene Inocencio, contact information provided	Joe Wray, contact information provided
Qualifications		They state that their team of certified engineers and analysts are experienced in HPE SimpliVity, Broadcom (VMWare), HPE Aruba, Fortinet firewalls, and Microsoft Servicer ecosystems, as well cloud platforms including Azure and AWS.	They say that they have provided infrastructure and support services since their founding in 2011. Their corporate background in rooted in HPE and Fortinet technologies, with a portfolio that includes VMware support, backup/disaster recovery and firewall management. They have experience in public sector collaboration.	They say they have over 20 years of experience in IT Infrastructure and Managed Services, and say they have over 50 completed projects since 2015, including municipalities.	They say that they have been in business for over 40 years and focus exclusively on disaster recovery and business resilience. They state that they have been recognized as a leader in the Gartner Magic Quadrant for DRaaS since 2014. They have technical certifications and compliance. They say that their staff has credentialed experts with deep experience in complex environments.
Historical Narrative of experience in providing Network Support Services.		They say that they have been providing Network Support Services to government, municipal, and public-sector organizations for over 22 years. They say their work spans all aspects of network infrastructure management including server and system administration, virtualization, cyber security, cloud integration, and business continuity planning.	They say they were founded in 2011 and have been delivering infrastructure services since then. They expanded their service portfolio in 2018 then they began providing SMS, and they also say they deployed the first HPE SimpliVity environment in the State of MI in 2018 (when working with the City of RH).	The evolved from a ISP into a company that provides software solutions and eventually into big data solutions. They state that they have over 20 years of IT Infrastructure and Managed Services experience.	They have been in business for over 40 years and exclusively provide true "end-to-end cyber resiliency, disaster recovery, and business continuity solutions".
Number of Years Providing Specific Service for Modules proposed: ICMS DRMS SMS FMS		ICMS - 15+ years DRMS - 10+ years SMS - 12+ years FMS - 14+ years	They do not explicitly state the years, however it seems that they may have provided ICMS, DRMS, and FMS since 2011 (their inception) and SMS since 2018.	They did not specifically answer this, but in reviewing their past performances, it could be implied as: ICMS: 13 years DRMS: 7 years FMS: 6 years SMS: unclear	They are only submitting a proposal for DRMS. Their company was founded in 1982 and originally provided off-site data storage, and then moved into focusing exclusively on disaster recovery and business resilience starting in 1999. DRMS: 26 years
List of Public Sector clients served, and corresponding modules		They have provided an extensive list of Michigan-based public entities including but not limited to: City of Rochester (ICMS, DRMS, SMS, FMS), Oakland County (ICMS, SMS, FMS), City of Clio (ICMS, SMS, FMS), City of Flushing (ICMS, DRMS, SMS, FMS), OPC (ICMS, DRMS, SMS, FMS), Crawford County (ICMS, DRMS, SMS, FMS), and SMART (DRMS). They have also provided an extensive list of non-Michigan public sector and federal agencies.	They provided the following: City of Farmington Hills/City of Farmington: ICMS, DRMS, FMS City of Rochester Hills: ICMS, DRMS, FMS, SMS L'Anse Creuse Public Schools: ICMS, DRMS, FMS	They provided the following public sector clients: City of Trenton, NJ: ICMS, DRMS, SMS, FMS County of Westchester, NY: ICMS	They stated: Since inception, Recovery Point has followed a corporate nondisclosure policy that restricts exposure of confidential client information for marketing. This includes publishing customer data in bid responses. Additional client information may be made available during the down-select process, subject to mutual agreement and the execution of appropriate
References		5 references provided, public-sector and municipal. They also provided performance evaluations in Appendix II.	3 references provided	5 references provided	3 references provided
Subcontractors		Yes. Infosys for Modules 1 & 2.	Yes. They will be using subcontractors for the following items: 24x7 SOC services for the compute infrastructure by **Kaseya** (utilizing Kaseya 365 User Pro licenses). Annual penetration testing by **Vonahai Security** as a "joint effort" between ITSG and Vonahai Security. **Kaseya Cloud** - Hosting the offsite cloud retention for the backup data.	They do not specifically state this, but they do state that they have 16 independent consultants as part of their workforce.	They will not be using any subcontractors

Network Support Services
RFP-RH-25-061
Proposals Opened: Wednesday, November 19, 2025 @ 3:00 p.m.

NAME ADDRESS	ATT	Global Solutions Group 31681 Dequindre Road Madison Heights, MI 48071	IT Solutions Group 28175 Haggerty Road Novi, MI 48377	Maestro Technologies, Inc. 1 West State Street, 3rd Floor Trenton, NJ 08608	Recovery Point Systems, Inc. 75 West Watkins Mill Rd. Gaithersburg, MD 20878
Detailed work plan & Methodology for each module proposed		**ICMS** - Onboarding & Baseline: Create an Infrastructure Baseline Document to inventory configurations, firmware, and health status for HPE SimpliVity, VMware vSphere, and Aruba switches. System Management: Perform regular health checks and manage the lifecycle of ESXi/vCenter and HPE firmware. Safe Upgrade Execution: All updates are first staged in the Disaster Recovery (DR) environment to verify stability and backup jobs before being applied to production. Monitoring: Automated monitoring tools to track CPU, memory, storage latency, and hardware status 24/7. **DRMS** - Architecture: Microsoft Azure-based solution that is immutable (WORM storage), air-gapped (logically isolated accounts), hosted entirely within the continental U.S. (CONUS). Migration Plan: Phased migration from the City's current HPE SimpliVity RapidDR to the new Azure environment, includes discovery, pilot testing, data seeding, and final cutover. Testing Cadence: Quarterly Partial Tests and an Annual Full DR Test. **SMS** - Vulnerability Management: Perform regular internal and WAN vulnerability scanning, assigning risk scores (Critical/High/Medium). Penetration Testing: Annual external and internal penetration tests, including footprint reconnaissance and simulated attacks to identify weak points. Risk & Policy: Perform gap analyses against City policies and maintain a "Risk Register" to track and close security gaps. Training: Includes phishing simulations and quarterly security workshops for City IT staff. **FMS** - Optimize the City's existing Fortinet FortiGate environment. Rule Optimization: Audit existing firewall rules to remove redundancies and enforce least-privilege access policies. Lifecycle Management: Quarterly firmware updates preceded by a configuration backup and compatibility check. Content Filtering: Manage web filtering and application control profiles to secure internet usage. Response: Guarantee a 30-minute response time for critical (P1) firewall incidents.	**ICMS**: They will monitor SimpliVity nodes and Omnistack software for performance and connectivity using HPE InfoSight, iLO, and SimpliVity management tools. SOC Integration: They plan to deploy Kaseya 365 Pro agents to the cluster to provide 24x7 Security Operations Center (SOC) monitoring for health and cyber threats. Update Strategy: Updates and upgrades will be coordinated with the City's team, typically scheduled for weekends or holidays, and performed in strict accordance with the SimpliVity interoperability guide to ensure compatibility. **DRMS**: They propose a phased migration to a new solution: Deployment: They will install a 24TB Datto SIRIS 6 BCDR appliance alongside the existing environment. Parallel Validation: A transition period where both systems run in parallel. They will test local/cloud restores, VM-level recovery, and instant virtualization to validate the new system. Steady State: Once validated, they will retire the old hardware and move to steady-state monitoring, which includes regular monthly reporting and annual full DR testing. **SMS**: Vulnerability Scanning: Using Kaseya VulScan for continuous authenticated and unauthenticated scans to detect OS and application-level vulnerabilities. Infrastructure Analysis: Use Network Detective Pro (agentless and agent-based) to document assets, analyze Active Directory health, and map network topology. Remediation: Integrate findings to prioritize risks using CVSS scoring and create targeted remediation plans. **FMS**: Centered on proactive management of the Fortinet perimeter. Continuous Operations: Includes 24x7 monitoring of health and traffic patterns, with rapid escalation for critical issues. Configuration Management: Regular reviews of firewall rules, NAT policies, and VPN configurations to optimize performance and security. Maintenance: Management of all firmware, signature, and security updates to protect against the latest threats.	**ICMS:** Startup - Analyze the HPE Simplivity, VMware, and Aruba environment to create an Infrastructure Baseline Document and integrate all assets into monitoring tools. Ongoing - Manage patch cycles (adhering to HPE/VMware update paths), optimize the 26 virtual servers, and provide 24x7 monitoring and troubleshooting . **DRMS:** Migration - Execute a 5-phase transition plan (Discovery, Build-Out, Data Migration, Testing, Cutover) to move from RapidDR to a SOC 2/FedRAMP certified cloud solution (AWS/Azure). Ongoing - Manage air-gapped, immutable backups and conduct quarterly tests and one annual full disaster recovery test . **SMS:** Startup - Assess the network to deliver a Security Policy Gap Analysis Report and establish a vulnerability baseline. Ongoing - Align with the NIST Cybersecurity Framework, perform monthly vulnerability scans, annual penetration testing, and facilitate annual incident response tabletop exercises . **FMS:** Startup - Conduct a Firewall Configuration Review to optimize existing Fortigate policies and rules. Ongoing - Manage firewall rules, content filtering, and firmware updates for Fortigate, FortiAnalyzer, and FortiMail appliances . They also say that they will be utilizing the ITIL Service Strategy for daily incident and service management. and that they employ Agile/Scrum methodologies (sprints, stand-ups) to ensure rapid delivery of projects like the DR migration.	**DRMS:** Project initiation - Formalize delivery team, assign experts, project kickoff call, confirm solution architecture, RACI review. Planning - Review critical path milestones, establish project timeline, client portal setup, and training. Implementation - Receive/install equipment, deploy network, configure backup repository, establish retention policies, set alerts/monitoring. Validation - End-to-end unit testing, validate solution is operational, acceptance testing. Steady State - Client in fully protected state, continuous backups/replication, annual test and DR event planning.
Assigned / Allocated Resources		They provided a cross-function team of 12 key personnel comprised of project managers, architects, engineers, and security analysts. They provided extensive resumes and a matrix breakdown of the allocated staffing resources.	The propose a team structure centered around a lead engineer, supported by a senior expert and the technical team. The support team will include 10 full time and 2 part time members. For the security team, they utilize the Kaseya SOC team which they say are available 24x7x365 for emergency service. Brief profiles were included for 2 members of the team.	They detailed the team member titles allocated for the project and what the duties would be on pages 13 & 14.	They say they will have a dedicated project manager to coordinate the implementation process, an account executive to be the primary interface for 12 months to ensure goals and budget priorities are met, and a technical staff to maintain and support ongoing operations.
Staff Profiles / Similar Work Performed		Provided in Appendix I: Resumes.	They shared narrative staff profiles for their lead engineer and the senior technical support.	They named 3 staff: Irene Inocencio, Akhila Andavolu, and Kamal Singh Bathla. They did not provide specific resumes/profiles or prior similar work.	They have provided many resumes in their Exhibit A which highlights key staff and relevant experience in DRMS.
Support Model					
In-House Support Staff available 24/7/365?		yes	They say that they do not offer 24x7x365 as a regular course of business, but they do offer 24/7 coverage in specific emergency or subcontracted capabilities.	They rely on a dispatch center and on-call rotation for after hours and weekends	They have a 24x7x365 toll-free line for client support. They also note that all clients also have access to the account manager and executive leadership team at any point.
Use overseas or off hours support?		GSG does not use any overseas or offshore resources. All technicians, engineers, and cybersecurity professionals are U.S.-based and CJIS/HIPAA-compliant. After-hours coverage is provided by their domestic on-call rotation, staffed from their Michigan technical operations center, ensuring full control, data security, and local accountability. If they need to use overseas augmentation it is solely to extend coverage not replace the primary US based support. When overseas staff are engaged, they have the same rigorous standards and background checks and they are logged and audited for compliance and accountability. Once the task window concludes all privilege is automatically disabled. It sounds as though they are not planning to use overseas resources for this project.	They say that neither they nor their subcontractors have overseas staff or overseas data centers.	While they state that the dedicated team for the City will be based out of Trenton, NJ, they have a significant workforce overseas. They do not state if the supports will come from overseas or not, just that weekend support is routed through dispatch center.	No, they have a 24/7/365 toll-free line for in-house support.

Network Support Services
RFP-RH-25-061
Proposals Opened: Wednesday,
November 19, 2025 @ 3:00 p.m.

NAME ADDRESS	ATT	Global Solutions Group 31681 Dequindre Road Madison Heights, MI 48071	IT Solutions Group 28175 Haggerty Road Novi, MI 48377	Maestro Technologies, Inc. 1 West State Street, 3rd Floor Trenton, NJ 08608	Recovery Point Systems, Inc. 75 West Watkins Mill Rd. Gaithersburg, MD 20878
Where is the closets support facility?		Their primary support facility is located in Madison Heights, MI. This proximity allows same-day onsite support and a 2–4-hour emergency response window for critical incidents. Additional engineering resources are available through a statewide network of on-call technicians positioned across southeast Michigan.	Novi, Michigan	Their closest facility is in Trenton, NJ, however they do state in their proposal that they will "set up a HelpDesk on-site at a designated location that will be covered by the resources that serve as IT Specialists and Network Domain management and support."	Maryland
Type of telephone support program and hours available:		24/7/365 Coverage: 24/7 Network Operations Center (NOC) and Security Operations Center (SOC) to handle support calls at any time, including nights, weekends, and holidays.	They do not utilize a traditional help desk call center, instead they propose direct contact with assigned team members during standard hours. They do have an emergency after hours solution through their SOC subcontracted team that is available after standard business hours.	They use a hybrid telephone support program that combines on-site coverage with a dispatch center for off-hours. Support Availability & Hours: 12 hours a day, 5 days a week (Mon–Fri). Weekend & After-Hours: Support during weekends and outside the primary 12-hour window is routed through a dispatch center rather than being answered directly by the active Help Desk team. Emergency Coverage: They provide 24/7/365 response for "Emergency" tickets (Priority 1), with a response goal of 1 hour.	Their toll-free line is staffed by in-house employees 24/7/365.
Procedures for handling routine, night, weekend and/or emergency calls:		Routine Calls (P3/P4) - will be logged through phone, email, or the service portal, depending on the method preferred by the City. These requests are typically addressed during extended business hours unless they are deemed urgent and require faster attention. All routine maintenance activities are scheduled and performed during standard maintenance windows to minimize service disruption. Night and Weekend Calls - Managed by the 24/7 Network Operations Center (NOC) and Security Operations Center (SOC) staff. Priority 1 (P1) and Priority 2 (P2) issues will be immediately escalated to ensure prompt resolution. Lower priority items will be placed in the service queue and addressed according to established procedures unless the City requests accelerated handling due to special circumstances. Emergency Calls (P1/P2) - In the event of an emergency, GSG's Emergency Response Protocol is activated immediately. An Incident Commander is assigned to coordinate all response efforts, and a dedicated conference bridge is initiated to maintain continuous communication. The City's leadership receives status updates every thirty to sixty minutes until the issue is resolved. Following resolution, a detailed post-incident report will be delivered within an agreed-upon timeframe.	Routine Calls - Mon-Fri 8am-8pm - Customers are instructed to directly contact their primary consultant or managing member via phone or email. Emergency Calls - Emergency service is available 24/7/365 via the Security Operation Center team with has a 30-minute SLA. Night & Weekend Support (non-emergency) - non-emergency work during nights and weekends is treated as a scheduled project.	Routine Calls (Business Hours) - Reception: Calls handled by the on-site Help Desk established at the City's location. All calls are immediately logged into the ticketing system. The workflow converts each ticket into either a "support call" or a "project task". Non-emergency tickets have a response goal of two (2) hours. The system logs resolutions until closure. Reporting and trend analytics are generated to allow for proactive rather than reactive work. Night & Weekend Calls (After-Hours) - Support calls are routed through a dispatch center rather than being answered directly by the primary Help Desk team. A Remote NOC Analyst is responsible for initial triage, system monitoring, and providing coverage for after-hours patches/updates. The NOC Analyst escalates issues to Level 2/Level 3 engineers based on severity. For non-critical issues (Priority 2, 3, & 4), the Time To Repair Goal clock stops during weekends and holidays. Emergency Calls (Priority 1) - Definition: Emergencies include site-down events, server outages, or degradation of critical resources. 24/7 response for emergency calls declared by the Business Administrator. Emergency tickets have a mandatory response time of within one (1) hour. The Time To Repair goal is 2 hours, and unlike routine calls, this clock continues running through weekends and holidays.	Routine, Night, and Weekend Calls: Since they maintain a 24x7x365 support center, the procedure for routine, night, and weekend calls remains consistent. Clients can contact support via the toll-free 800 number or the client portal. Level 1 Support (Service Desk): These inquiries are handled by the always present hosting team (Level 1) which is staffed continuously. Tracking: All incidents and work are tracked in their support ticketing system. Emergency Calls: For critical emergencies, specifically declaring a disaster to initiate recovery; explicitly inform RPS that you are declaring a Disaster by calling the telephone number RPS provides, based on severity and complexity, incidents are assigned to Level 2 (Technical Engineering) or Level 3 (Senior Technical Engineering) support, clients have full access to the Account Manager and Executive Leadership Team at any point for escalation.
Do consultants have ability to work remotely? What is the process if so?		All engineers performing remote work is required to connect through a City-approved VPN or ZTNA solution, both of which must web authenticated using MFA, and all privileged operations will be routed through approved PAM gateways. All endpoints used for remote work must be fully encrypted, monitored using EDR tools, and compliant with the City's cybersecurity standards.	Yes, consultants typically work remotely. They detailed a specific Hybrid PAM framework which includes mandatory MFA enforcement for all remote access and VPN connections, JIT access that is only granted for specific tasks and limited durations, role based controls with least privilege principals. All remote and privileged activity is logged, monitored, and integrated with SIEM platforms.	Yes, they have the ability for remote support and work. SSL VPN: Consultants utilize SSL VPN for secure remote connections. Remote Desktop: Remote Desktop Connection utilizing Microsoft Terminal Service Technology to access systems. Dispatch Center: For weekend and after-hours support, the process involves routing calls through a dispatch center to remote technicians rather than on-site staff	Yes. Remote work is delivered through an Assisted Service-Level specific to implementation and service delivery, which is defined in standard RACI (Responsible, Accountable, Consulted, Informed) documentation. Initial Deployment: Certified experts from Recovery Point assist remotely with the initial deployment and configuration required to implement the disaster recovery solution. Knowledge Transfer: During the initial phase, the team provides knowledge transfer to the client's staff engaged in the deployment. Ongoing Support: After implementation, they assist remotely with change management and troubleshooting of any performance impacts or service outages related to the infrastructure.

Network Support Services
RFP-RH-25-061
Proposals Opened: Wednesday,
November 19, 2025 @ 3:00 p.m.

NAME	ATT	Global Solutions Group	IT Solutions Group	Maestro Technologies, Inc.	Recovery Point Systems, Inc.
ADDRESS		31681 Dequindre Road Madison Heights, MI 48071	28175 Haggerty Road Novi, MI 48377	1 West State Street, 3rd Floor Trenton, NJ 08608	75 West Watkins Mill Rd. Gaithersburg, MD 20878
Policy for privileged access to the City's on-premise and cloud environment?		Their model enforces least privilege access for all administrative functions, allowing engineers to perform only the specific tasks necessary for their roles. All privileged credentials are stored in a PAM vault. GSG says they also hold up stringent separation of duties across key operational domains. Access privileges undergo quarterly re-certifications.	Unified RBAC: Privileged access is provisioned based on clearly defined roles and least-privilege principles, applied consistently across on-prem systems (like Active Directory) and cloud platforms (like Azure) Just-In-Time (JIT) Privilege Elevation: Administrative rights are not permanent. They are granted only for specific tasks and limited durations to reduce persistent exposure. MFA Enforcement: MFA is mandatory for all privileged access, including VPN/remote access, administrative consoles, and cloud portals. Credential Vaulting: Privileged credentials are stored in a secure vault with encrypted access and automated rotation. Logging and Monitoring: All privileged activities are logged, monitored, and available for integration with SIEM platforms. Logs capture session details, commands, and configuration changes. Quarterly Access Reviews: Perform periodic access certifications every quarter to ensure accounts remain necessary and compliant, promptly removing any orphaned or outdated accounts . Change Management: Any task requiring elevated rights is executed under change control with documented authorization and rollback procedures	All Maestro personnel providing services must undergo an background check which includes fingerprinting and drug testing. If required, personnel will receive City-provided photo identification badges. Role-Based Access Control (RBAC): generated for all servers, routers, and operating components. This ensures that permissions are assigned based on specific roles rather than generic administrative access . Password Management: collecting and documenting Admin/Root passwords on the server sides. Secure Storage: sensitive credentials and access details will be documented and placed within a secure method. All access configurations are formalized in an "Operational Guidebook" created by Maestro to track all devices/systems added, moved, or reconfigured, network diagrams including IP and MAC addresses, device naming and addressing conventions established by the City . Remote Access - Secure Channels: Remote access for privileged tasks is conducted via SSL VPN or Remote Desktop Connection (RDC) utilizing Microsoft Terminal Service Technology.	They say that as a DR provider, they do not require privileged access within the City's production environment and that all privileged activity within the Recovery Point environment supporting the City is fully secure.
Confirm mandatory use of MFA for all administrative access		MFA is mandatory for connecting to City servers, VMWare/Broadcom consoles, firewall management consoles, backup and DR portals, and cloud-hosted SaaS platforms, as well as any privileged VPN or ZTNA session. Approved MFA options include DUO Security, Microsoft Authenticator, and F1DO2-compliant hardware keys. Mobile-based push notifications and Time-Based one-Time Password (TOTP) mechanisms.	MFA Enforcement: MFA is mandatory for all privileged access, including VPN/remote access, administrative consoles, and cloud portals.	They did not include this in their proposal.	They say they understand and can meet this requirement.
Describe use of Just-In-Time of ephemeral credentials to minimize the duration of privileged access		JIT privileges will be granted strictly on an as-needed basis rather than being permanently assigned. Once the approved change window is completed, access is automatically revoked to prevent misuse or prolonged exposure of sensitive systems. The JIT Access Model is managed through a PAM system.	Just-In-Time (JIT) Privilege Elevation: Administrative rights are not permanent. They are granted only for specific tasks and limited durations to reduce persistent exposure.	This was not included in their proposal.	They did not include this in their proposal.
Confirm that all privileged remote sessions are monitored and logged		All privileged sessions, remote or local, will be recorded using either video capture or keystroke logging depending on the system's capabilities. Sessions will be tagged and logged. Recorded session data will be forwarded to the SIEM system for centralized analysis and alerting as well as reviewed as part of a weekly operational security reviews to identify anomalies or policy violations.	Logging and Monitoring: All privileged activities are logged, monitored, and available for integration with SIEM platforms. Logs capture session details, commands, and configuration changes.	They do not explicitly confirm content or actions taken by a technician during PAM is recorded or logged during remote sessions. They state that they do log tickets.	
For any security incident or data breach occurring within the vendor's managed service platform or affecting City data/systems, the vendor shall be contractually obligated to provide mandatory notification within 1 hour of discovery by both phone and email.		Within 1 hour, a phone call will be made to the City's primary and secondary contacts to ensure immediate awareness. An email with an initial summary of the incident will follow along with the activation of an incident response bridge. Within 4 hours they will focus on immediate containment steps to prevent further impact and a preliminary impact assessment will be prepared to provide the scope and severity. Within 5 business days they will deliver a detailed incident report documenting findings, actions taken, and outcomes. It will also include a root cause analysis, as well as recommendations to prevent future occurrence and enhance overall security.	They simply sated "agreed"	Their SLA for Emergency Tickets Priority 1 does state that they will be responded to within 1 hour, however they do not mention phone and email.	
Did the vendor provide a guarantee that all vendor-managed laptops, workstations, or servers used by personnel to access the City's network have mandator and up-to-date security protocols, including EDR or next-gen anti-virus, and a managed host firewall.		They say that all devices will be equipped with centrally managed Next-Generation Antivirus and EDR solutions, such as CrowdStrike, providing advanced malware protection and continuous monitoring and that each device employs full disk encryption using AES-256 or stronger algorithms to safeguard stored data from unauthorized access. Additionally, a managed host firewall is configured with a default-deny baseline, allowing only approved network traffic, other security policies include strict USB and peripheral device controls, removal of local administrative rights for engineers, and strict asset inventory management with detailed audit logs and devices automatically lock after a period of inactivity, and remote wipe capabilities are enabled to protect data in case of loss or theft.	They state that they use the latest in antivirus and EDR and that they enforce MFA and PAM.	They do not explicitly state this in their proposal.	They say they will not be accessing the City's network.
Provide a guarantee that when a support issue arises for a service you are providing, your firm will find the necessary expertise to resolve the issue at no additional cost to the City, even if it requires seeking outside assistance.		They contractually guarantee that any support issue within the agreed scope of services will be resolved at no additional cost to the City, even when it requires highly specialized or external expertise. If an incident, defect, or complex configuration issue arises in ICMS, DRMS, SMS, or FMS, GSG will: Assign internal SMEs to drive root-cause analysis and remediation; Escalate to higher-tier GSG architects and our OEM/partner ecosystem as needed; Absorb the cost of any additional specialists required to resolve the issue, so long as the work is within the contracted scope (i.e., not a City-requested enhancement or new	They said they will work to resolve the issue and reach out to experts as needed	They do not explicitly state this in their proposal.	They say they understand and can meet this requirement.

Network Support Services
RFP-RH-25-061
Proposals Opened: Wednesday,
November 19, 2025 @ 3:00 p.m.

NAME ADDRESS	ATT	Global Solutions Group 31681 Dequindre Road Madison Heights, MI 48071	IT Solutions Group 28175 Haggerty Road Novi, MI 48377	Maestro Technologies, Inc. 1 West State Street, 3rd Floor Trenton, NJ 08608	Recovery Point Systems, Inc. 75 West Watkins Mill Rd. Gaithersburg, MD 20878
For each module proposed, provide a list of proposed Service Level Agreements:		They have provided this on page 91 & 92 (numbered pgs 82 & 83) in their proposal.	They did not supply itemized SLAs but say they are "confident that they can meet the described SLA's in the RFP".	They did not provide performance-based SLAs specific to the individual functions of each module. They did provide a standard support ticket SLA that focused solely on response and repair times on page 15.	They say they provide SLAs attached to the MSA as Statements of Work and are solution specific customized. They provided this in Exhibit B.
For each module proposed, outline key metrics and information that will be included in the monthly performance reports:		**ICMS** – Operational Reliability: Tracks system uptime percentages and compares them directly against Service-Level Agreements (SLAs). Incident Management: Provides a statistical breakdown of incidents by severity (P1–P4), monitors operational responsiveness. Security & Compliance: Evaluates patch compliance across all classification levels (critical, high, medium, low). Resource Capacity: Monitors trends in CPU, memory, and storage usage. Change & Risk Analysis: Summarizes major configuration updates (Change Management) and concludes with identified risks and strategic recommendations. **DRMS** – Backup Reliability: Detailed tracking of backup success and failure rates across every system and data tier. Recovery Performance: Validation of disaster recovery effectiveness by comparing actual results against defined RPO and RTO targets. Restoration Efficiency: Analysis of real-world restore events, monitoring their frequency and duration. Resilience & Compliance: A summary of periodic DR test outcomes. Capacity Planning: Review of DR storage utilization and growth trends. **SMS** – Vulnerability Management: A breakdown of vulnerability counts by severity level. Incident Response: Tracks trends in security incidents (P1–P3) and their resolution times. Threat Intelligence: Analyzes patterns in threat detections and anomalous activity. Compliance & Governance: Summarizes key activities such as policy reviews, assessments, and audits. User Awareness: Metrics on training and user engagement. **FMS** – Network Availability: Tracks firewall uptime and performance analytics. Change Control: A detailed review of rule change logs—covering standard, emergency, and rollback changes. Threat Detection: Analyzes data from Intrusion Prevention (IPS) events, URL filtering, and geo-blocking activities. System Maintenance: Verifies firmware versions and subscription statuses. Traffic Analysis: Identifies high-risk or anomalous traffic patterns.	**ICMS** - System Health: Server, storage, and network uptime; hypervisor/cluster performance (CPU, memory, IOPS). Capacity: Storage and backup repository utilization trends; capacity planning for compute and cloud resources. Hardware: Critical hardware alerts. Patching: Patch compliance rates for OS and firmware; deployment timelines and exceptions. **DRMS** - Performance: Backup job success/failure rates; RPO and RTO achievement metrics against service levels. Validation: Periodic restore testing and validation reports; cloud replication and retention compliance. **SMS** - Threat Monitoring: IPS/IDS and endpoint security events; account lockouts and anomaly detection. Vulnerability Management: Vulnerability counts by severity (Critical, High, Medium, Low); remediation progress and time-to-remediate (MTTR). Identity & Access: Privileged account usage audits; MFA adoption metrics; inactive/orphaned account identification. **FMS** - Traffic & Threats: Top blocked threats and suspicious patterns; bandwidth utilization by application/department. Operations: Firewall rule changes and approvals (audit trail); VPN session monitoring. **All Modules** - Operational: Incident volume and resolution times; SLA compliance reporting. Compliance: Policy adherence tracking (passwords, encryption); audit readiness summaries. Executive Summary: High-level analysis of environment stability, risk posture, and strategic recommendations.	**ICMS** Information Included: Monthly reports covering the health and performance of all infrastructure components. Service Delivery Manager: Responsible for delivering infrastructure uptime reports. **DRMS** Information Included: Monthly reporting on backup status and health. Key Metrics: The Cloud DR Architect is specifically tasked with providing monthly RPO/RTO reporting. **SMS** Information Included: Vulnerability Scanning: Reports will include alerts and reporting. Policy Assessment: Regular reporting on Network Services Security Policy Assessments. Remediation: Reports and remediation plans generated by the Security Analyst. **FMS** Information Included: monitoring and Firewall Management and Rules Analysis In addition to the module-specific technical data, they outlined a standard format for engagement compliance reports, which will include: Name of the person responsible for delivery. Amount of time spent on the project. Status of the project presented as a RAG report (Red, Amber, Green) indicating challenges, risks, and completion status. Help Desk Trends: Trend analysis graphs showing ticket volume, open/closed status, and ticket types .	Standard Monthly Performance Reporting Sources: Monthly SLA reports: Measuring actual performance against contract goals. Service desk ticketing analysis: Tracking incident volume and resolution. Portal client escalation records: Monitoring escalated issues. RPS portal request question review: Analyzing client inquiries. Customer surveys: Gauging overall satisfaction. They also list specific technical metrics that they track to ensure performance: Recovery RTO/RPO metrics Backup success rates Data transfer volumes DR Test Execution Orchestration Post-mortem DR Testing goals RPS dark fiber network uptime Facility uptime
Attachment C Cost Proposal - see cost summary tab		see cost summary tab	see cost summary tab	see cost summary tab	See Cost Summary Tab
Attachment B Contract Exceptions		none	none	none	Yes - they supplied just over a page of exceptions with their proposal and Attachment B page.

After review of the submitted proposals, ATT has been deemed non-responsive.

RFP-RH-25-061
Network Support Services
Cost Summary

	Global Solutions Group										
Managed Service Module	**Months**	**Monthly Fee Year 1**	**Total Fee Year 1**	**Monthly Fee Year 2**	**Total Fee Year 2**	**Monthly Fee Year 3**	**Total Fee Year 3**	**Monthly Fee Year 4**	**Total Fee Year 4**	**Monthly Fee Year 5**	**Total Fee Year 5**
Infrastructure Co-Management Service (ICMS)	12	$ 9,600.00	$ 115,200.00	$ 9,888.00	$ 118,656.00	$ 10,184.64	$ 122,215.68	$ 10,490.18	$ 125,882.16	$ 10,804.89	$ 129,658.68
Disaster Recovery Managed Service (DRMS)	12	$ 7,450.00	$ 89,400.00	$ 7,673.50	$ 92,082.00	$ 7,903.71	$ 94,844.52	$ 8,140.81	$ 97,689.72	$ 8,385.04	$ 100,620.48
Security Managed Service (SMS)	12	$ 5,750.00	$ 69,000.00	$ 5,922.50	$ 71,070.00	$ 6,100.18	$ 73,202.16	$ 6,283.18	$ 75,398.16	$ 6,471.68	$ 77,660.16
Firewall Managed Service (FMS)	12	$ 3,800.00	$ 45,600.00	$ 3,914.00	$ 46,968.00	$ 4,031.42	$ 48,377.04	$ 4,152.36	$ 49,828.32	$ 4,276.93	$ 51,323.16
		Year 1	**$ 319,200.00**	**Year 2**	**$ 328,776.00**	**Year 3**	**$ 338,639.40**	**Year 4**	**$ 348,798.36**	**Year 5**	**$ 359,262.48**

Initial Startup Costs	**Estimated Hours**	**Hourly Rate**	**Total Cost**
Initial Startup for Infrastructure Co-Management Service (ICMS)	100	$ 115.00	$ 11,500.00
Initial Startup for Disaster Recovery Managed Service (DRMS)	80	$ 115.00	$ 9,200.00
Initial Startup for Security Managed Service (SMS)	40	$ 115.00	$ 4,600.00
Initial Startup for Firewall Managed Service (FMS)	40	$ 95.00	$ 3,800.00
		Total Startup Costs (Year 1 Only)	**$ 29,100.00**

Total Cost	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Contract Grand Total**
	$ 348,300.00	$ 328,776.00	$ 338,639.40	$ 348,798.36	$ 359,262.48	$ 1,723,776.24
			Total 3-Year Contract Cost	**$ 1,015,715.40**		
					Total 5-Year Contract Cost	**$ 1,723,776.24**

Ad-Hoc Services Rate Schedule

Labor Category:	Hourly Rate 8am-5pm M-F	Hourly Rate After 5pm M-F	Hourly Rate Weekends/ Holidays
Senior Project Manager	$ 110.00	$ 130.00	$ 130.00
Infrastrucutre Architect	$ 130.00	$ 150.00	$ 150.00
Cybersecurity Architect	$ 130.00	$ 150.00	$ 150.00
Senior Penetration Tester	$ 130.00	$ 150.00	$ 150.00
Disaster Recover Engineer	$ 115.00	$ 130.00	$ 130.00
System Administrator	$ 95.00	$ 115.00	$ 115.00
Network Engineer	$ 85.00	$ 100.00	$ 100.00
Network Administrator	$ 75.00	$ 90.00	$ 90.00
IT Helpdesk Engineer	$ 54.00	$ 70.00	$ 70.00
Backup Administrator	$ 110.00	$ 120.00	$ 120.00

RFP-RH-25-061
Network Support Services
Cost Summary

						IT Solutions Group					
Managed Service Module	**Months**	**Monthly Fee Year 1**	**Total Fee Year 1**	**Monthly Fee Year 2**	**Total Fee Year 2**	**Monthly Fee Year 3**	**Total Fee Year 3**	**Monthly Fee Year 4**	**Total Fee Year 4**	**Monthly Fee Year 5**	**Total Fee Year 5**
Infrastructure Co-Management Service (ICMS)	12	$ 8,800.00	$ 105,600.00	$ 8,800.00	$ 105,600.00	$ 8,800.00	$ 105,600.00	$ 9,250.00	$ 111,000.00	$ 9,250.00	$ 111,000.00
Disaster Recovery Managed Service (DRMS)	12	$ 4,600.00	$ 55,200.00	$ 4,600.00	$ 55,200.00	$ 4,600.00	$ 55,200.00	$ 4,950.00	$ 59,400.00	$ 4,950.00	$ 59,400.00
Security Managed Service (SMS)	12	$ 5,600.00	$ 67,200.00	$ 5,600.00	$ 67,200.00	$ 5,600.00	$ 67,200.00	$ 5,900.00	$ 70,800.00	$ 5,900.00	$ 70,800.00
Firewall Managed Service (FMS)	12	$ 1,850.00	$ 22,200.00	$ 1,850.00	$ 22,200.00	$ 1,850.00	$ 22,200.00	$ 2,150.00	$ 25,800.00	$ 2,150.00	$ 25,800.00
		Year 1	**$ 250,200.00**	**Year 2**	**$ 250,200.00**	**Year 3**	**$ 250,200.00**	**Year 4**	**$ 267,000.00**	**Year 5**	**$267,000.00**

Initial Startup Costs	**Estimated Hours**	**Hourly Rate**	**Total Cost**
Initial Startup for Infrastructure Co-Management Service (ICMS)	20	$ 105.00	$ 2,100.00
Initial Startup for Disaster Recovery Managed Service (DRMS)	30	$ 115.00	$ 3,450.00
Initial Startup for Security Managed Service (SMS)	10	$ 105.00	$ 1,050.00
Initial Startup for Firewall Managed Service (FMS)	5	$ 105.00	$ 525.00
		Total Startup Costs (Year 1 Only)	**$ 7,125.00**

Total Cost	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Contract Grand Total**
	$ 257,325.00	$ 250,200.00	$ 250,200.00	$ 267,000.00	$ 267,000.00	$ 1,291,725.00

Total 3-Year Contract Cost	**$ 757,725.00**
Total 5-Year Contract Cost	**$ 1,291,725.00**

Ad-Hoc Services Rate Schedule

Labor Category:	Hourly Rate 8am-5pm M-F	Hourly Rate After 5pm M-F	Hourly Rate Weekends/ Holidays
Enterprise Services - Infrastructure, Firewall, Security, DRMS, Networking	$ 115.00	$ 135.00	$ 210.00
Client - Desktop, Notebook, Printer, Training	$ 80.00	$ 95.00	$ 110.00

Maestro Technologies, Inc.

Managed Service Module	Months	Monthly Fee Year 1	Total Fee Year 1	Monthly Fee Year 2	Total Fee Year 2	Monthly Fee Year 3	Total Fee Year 3	Monthly Fee Year 4	Total Fee Year 4	Monthly Fee Year 5	Total Fee Year 5
Infrastructure Co-Management Service (ICMS)	12	$ 3,980.00	$ 47,760.00	$ 4,059.60	$ 48,715.20	$ 4,140.79	$ 49,689.48	$ 4,223.61	$ 50,683.32	$ 4,308.08	$ 51,696.96
Disaster Recovery Managed Service (DRMS)	12	$ 3,310.00	$ 39,720.00	$ 3,376.20	$ 40,514.40	$ 3,443.72	$ 41,324.64	$ 3,512.60	$ 42,151.20	$ 3,582.85	$ 42,994.20
Security Managed Service (SMS)	12	$ 3,910.00	$ 46,920.00	$ 3,988.20	$ 47,858.40	$ 4,067.96	$ 48,815.52	$ 4,149.32	$ 49,791.84	$ 4,232.31	$ 50,787.72
Firewall Managed Service (FMS)	12	$ 4,210.00	$ 50,520.00	$ 4,294.20	$ 51,530.40	$ 4,380.08	$ 52,560.96	$ 4,467.69	$ 53,612.28	$ 4,557.04	$ 54,684.48
		Year 1	**$ 184,920.00**	**Year 2**	**$ 188,618.40**	**Year 3**	**$ 192,390.60**	**Year 4**	**$ 196,238.64**	**Year 5**	**$ 200,163.36**

Initial Startup Costs	Estimated Hours	Hourly Rate	Total Cost
Initial Startup for Infrastructure Co-Management Service (ICMS)	18	$ 110.00	$ 1,980.00
Initial Startup for Disaster Recovery Managed Service (DRMS)	16	$ 110.00	$ 1,760.00
Initial Startup for Security Managed Service (SMS)	14	$ 115.00	$ 1,610.00
Initial Startup for Firewall Managed Service (FMS)	12	$ 120.00	$ 1,440.00
		Total Startup Costs (Year 1 Only)	**$ 6,790.00**

Total Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Contract Grand Total
	$ 191,710.00	$ 188,618.40	$ 192,390.60	$ 196,238.64	$ 200,163.36	$ 969,121.00

Total 3-Year Contract Cost	**$ 572,719.00**
Total 5-Year Contract Cost	**$ 969,121.00**

Ad-Hoc Services Rate Schedule

Labor Category:	Hourly Rate 8am-5pm M-F	Hourly Rate After 5pm M-F	Hourly Rate Weekends/ Holidays
L1/L2 NOC/Help Desk	$ 50.00	$ 65.00	$ 75.00
System Admin (L2/L3)	$ 95.00	$ 120.00	$ 145.00
Aruba Network Engin	$ 115.00	$ 140.00	$ 165.00
Sen VMware/Simplivity Engin.	$ 125.00	$ 150.00	$ 175.00
Backup/DR Specialist	$ 95.00	$ 120.00	$ 145.00
Security Analyst	$ 105.00	$ 135.00	$ 160.00
Penetration Tester	$ 165.00	$ 195.00	$ 220.00
Fortinet Firewall Eng	$ 130.00	$ 160.00	$ 185.00
Wireless Enginer	$ 105.00	$ 135.00	$ 160.00
Service Del Manager	$ 85.00	$ 110.00	$ 130.00
Account Manager	$ 65.00	$ 80.00	$ 95.00

						Recovery Point Systems Inc.					
Managed Service Module	**Months**	**Monthly Fee Year 1**	**Total Fee Year 1**	**Monthly Fee Year 2**	**Total Fee Year 2**	**Monthly Fee Year 3**	**Total Fee Year 3**	**Monthly Fee Year 4**	**Total Fee Year 4**	**Monthly Fee Year 5**	**Total Fee Year 5**
Infrastructure Co-Management Service (ICMS)	12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Disaster Recovery Managed Service (DRMS)	12	$ 14,096.00	$ 169,152.00	$ 14,096.00	$ 169,152.00	$ 14,096.00	$ 169,152.00	$ 14,096.00	$ 169,152.00	$ 14,096.00	$ 169,152.00
Security Managed Service (SMS)	12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Firewall Managed Service (FMS)	12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		Year 1	**$ 169,152.00**	**Year 2**	**$ 169,152.00**	**Year 3**	**$ 169,152.00**	**Year 4**	**$ 169,152.00**	**Year 5**	**$ 169,152.00**

Initial Startup Costs	**Estimated Hours**	**Hourly Rate**	**Total Cost**
Initial Startup for Infrastructure Co-Management Service (ICMS)	0	$ -	$ -
Initial Startup for Disaster Recovery Managed Service (DRMS)	0	$ -	$ 14,287.00
Initial Startup for Security Managed Service (SMS)	0	$ -	$ -
Initial Startup for Firewall Managed Service (FMS)	0	$ -	$ -
		Total Startup Costs	**$ 14,287.00**

Total Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Contract Grand Total
	$ 183,439.00	$ 169,152.00	$ 169,152.00	$ 169,152.00	$ 169,152.00	$ 860,047.00

Total 3-Year Contract Cost	**$ 521,743.00**
Total 5-Year Contract Cost	**$ 860,047.00**

Ad-Hoc Services Rate Schedule

Labor Category:	Hourly Rate 8am-5pm M-F	Hourly Rate After 5pm M-F	Hourly Rate Weekends/ Holidays
Operational Support	$ 200.00	$ 225.00	$ 225.00
Professional Services	$ 200.00	$ 225.00	$ 225.00

						ATT					
Managed Service Module	**Months**	**Monthly Fee Year 1**	**Total Fee Year 1**	**Monthly Fee Year 2**	**Total Fee Year 2**	**Monthly Fee Year 3**	**Total Fee Year 3**	**Monthly Fee Year 4**	**Total Fee Year 4**	**Monthly Fee Year 5**	**Total Fee Year 5**
Infrastructure Co-Management Service (ICMS)	12	$ 17,999.00	$ 215,988.00	$ 17,999.00	$ 215,988.00	$ 17,999.00	$ 215,988.00	$ 17,999.00	$ 215,988.00	$ 17,999.00	$ 215,988.00
Disaster Recovery Managed Service (DRMS)	12	$ -	$ -		$ -	$ -	$ -	$ -	$ -	$ -	$ -
Security Managed Service (SMS)	12	$ 13,400.00	$ 160,800.00	$ 13,400.00	$ 160,800.00	$ 13,400.00	$ 160,800.00	$ 13,400.00	$ 160,800.00	$ 13,400.00	$ 160,800.00
Firewall Managed Service (FMS)	12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		Year 1	**$ 376,788.00**	**Year 2**	**$ 376,788.00**	**Year 3**	**$ 376,788.00**	**Year 4**	**$ 376,788.00**	**Year 5**	**$ 376,788.00**

Initial Startup Costs	**Estimated Hours**	**Hourly Rate**	**Total Cost**
Initial Startup for Infrastructure Co-Management Service (ICMS)	350	$ 51.00	$ 17,850.00
Initial Startup for Disaster Recovery Managed Service (DRMS)	0	$ -	
Initial Startup for Security Managed Service (SMS)	180	$ 57.00	$ 10,260.00
Initial Startup for Firewall Managed Service (FMS)	180	$ 50.00	$ 9,000.00
		Total Startup Costs (Year 1 Only)	**$ 37,110.00**

Total Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Contract Grand Total
	$ 413,898.00	$ 376,788.00	$ 376,788.00	$ 376,788.00	$ 376,788.00	$ 1,921,050.00

Total 3-Year Contract Cost	**$ 1,167,474.00**
Total 5-Year Contract Cost	**$ 1,921,050.00**

Ad-Hoc Services Rate Schedule

Labor Category:	Hourly Rate 8am-5pm M-F	Hourly Rate After 5pm M-F	Hourly Rate Weekends/ Holidays
Operational Support	$ 200.00	$ 225.00	$ 225.00
Professional Services	$ 200.00	$ 225.00	$ 225.00

*Non-Resposive for failure to respond to RFP requirements

RFP-RH-25-061					
Network Support Services					
Contract Cost Total Summary					
	Global Solutions Group	IT Solutions Group	Maestro Technoligies, Inc.	Recovery Point Systems	ATT
3 Year Contract Cost Total	$ 1,015,715.40	$ 757,725.00	$ 572,719.00	$ 521,743.00	$ 1,167,474.00
				*Did not propose all	*Non-responsive
				only DRMS	