Proposal

Phase 2 and 3: Computer-Aided Dispatch Performance Remediation and Services

December 29, 2021

Fulton County, Georgia

MissionCriticalPartners

Table of Contents

Introduction Letter

December 29, 2021

Glenn Melendez, Chief Information Officer
Department Relations
Fulton County IT
141 Pryor Street
Atlanta, GA 30303

Re: CAD Performance Remediation and Services

Dear Mr. Melendez,

Mission Critical Partners, LLC (MCP) is pleased to provide Fulton County, GA (County) with this proposal for remediation costs and support services that we believe will significantly enhance the system's reliability and greatly improve system and infrastructure support. The foundation of this proposal is the Public Safety System Network Assessment performed by MCP the week of September 30, 2019, in addition to the knowledge gained through support of the environment.

Our assessment generated multiple findings and recommendations, which we have prioritized into a two-phased approach. These phases are prioritized by speed to execute and impact. In our proposal, we have identified the remediation tasks and associated costs necessary to reduce the number of disruptions and to enhance the ability to correct any disruption more expeditiously.

If you have any questions about the assessment report or the contents of this proposal, please contact Chris Faircloth. His contact information follows:

Chris Faircloth
Mission Critical Partners, LLC
690 Grays Woods Blvd.
Port Matilda, PA 16870

Cell: 321.848.2273
Office: 321.866.8779
Email: ChrisFaircloth@MissionCriticalPartners.com

On behalf of our entire team, we stand behind Fulton County to serve as your partner and your advocate.

Sincerely,

Mission Critical Partners, LLC

David S. Jones, President
Lifecycle Management Services Division

About Mission Critical Partners

At MCP, Our Mission Is Simple: To Improve Emergency Response and Justice Outcomes

We are committed to working collaboratively with you to implement successful solutions for your networks, data, and operations. More than just a consultant, we act as trusted advisors to our clients, striving to deliver value, efficiency, and fresh ideas—all while mitigating risk. We are solely focused on the public safety, justice, healthcare and critical communications sectors, and what makes us different is our holistic perspective. A leading provider of data integration, consulting, network and cybersecurity services, our vision is to transform the mission-critical communications and public-sector networks and operations into integrated ecosystems.

More importantly, we stand behind the significance of the work our clients do and how critical their missions are—not just for their organizations, but because their communities are counting on them. While we are proud to have the largest, most experienced team of specialized experts in the industry, our greatest pride comes from applying this expertise to work side by side with our clients to implement the best possible solutions—because the mission matters.

By the Numbers

- Since 2009, MCP has supported 2,200+ projects for 750+ public-sector and critical communications agencies
- We serve clients in 48 states and 95% of the nation's largest metropolitan areas
- Our staff consists of 150+ subject-matter experts (SMEs), each with an average of 25 years of experience, dedicated to supporting our clients and their missions
- We create significant project cost savings for our clients—often 15%, sometimes more
- More than 90% of our clients remain with us from project to project

BECAUSE
THE MISSION
MATTERS

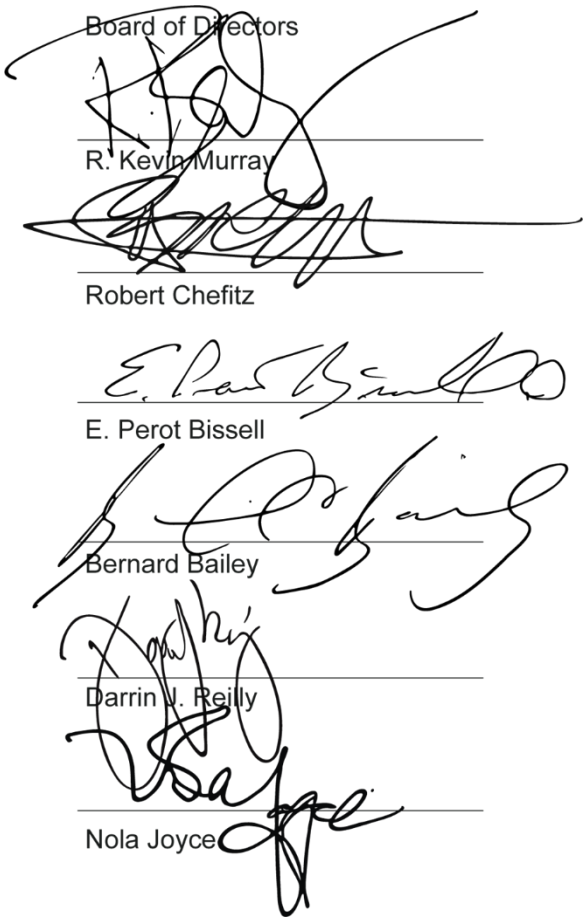
MissionCriticalPartners

We’re Committed to Putting our Clients First

Partnering with a firm that brings an independent, objective perspective to every engagement is a top priority of our clients. We stand behind our commitment to always put the fundamental interests of our clients first.

From our inception, vendor-neutrality is a value that underpins every aspect of what we do. Our goal is to determine the most favorable solution for our clients based on their unique requirements, budget, governance structure, operations, and existing technologies. We provide a holistic perspective regarding the entire mission-critical communications ecosystem, free of bias or favoritism to any specific product or service provider. Our recommendations always are based solely on the value and the benefit provided to the client.

For clients, this approach means more control and greater visibility into the systems they ultimately are responsible for operating and maintaining, and—more importantly—a successful project that improves outcomes.



Statement of Services

Executive Summary

The executive summary section of this proposal is intended to provide a summary version of the recommended remediation tasks and their benefits. All services listed here are described in detail within the proposed scope of work.

Phase 1: VMWare Environment Replacement Recommendation

Deploy dedicated hardware for the public safety environment, which includes the following servers:

Production Servers	Training Servers	Testing Servers	DMZ Servers
VMWP-RMSCDAP01	VMWT-RMSCDAP01	VMWR-RMSCDAP01	VSWP-RMSCDAP01
VMWP-RMSCDAP02	VMWT-RMSCDAP02	VMWR-RMSCDAP02	VSWP-RMSCDAP02
VMWP-RMSCDAP03	VMWT-RMSCDAP05	VMWR-RMSCDDB01	VSWP-RMSCDAP03
VMWP-RMSCDAP04	VMWT-RMSCDDB01		VSWT-RMSCDAP01
VMWP-RMSCDAP05			
VMWP-RMSCDAP06			
VMWP-RMSCDAP08			
VMWP-RMSCDAP09			
VMWP-RMSCDDB01			
VMWP-RMSCDDB03			
Vmwp-nmotnap01			
Vmwp-nmotnap02			

These servers include the following applications:

Applications	
• Computer-aided dispatch (CAD) • Crystal reports • Continuous Service Manager (CSM) • Freedom • Message switch • Mobile Communications Terminal (MCT) • Mobile Data System (MDS) • Mobile Field Reporting • Moblan	• Operational Program Software (OPS) • Push-to-Conference (P2C) • PageGate • ProQA • Records management system (RMS) • Short Message Service (SMS) • Structured Query Language (SQL) • GEARS • HigherGround

The benefits are listed below:

- Reduced outage duration and frequency
- Best practices for public safety systems
- Eliminate resource contention

Note: As recommended in the *Public Safety System Network Assessment Report, September 2019 for Fulton County (County), Georgia (hereinafter referred to as Assessment Report)*, Section 4.1.1 VMWare Environment:

> *Public safety networks should not share hosts with other servers to prevent issues with other servers causing performance issues with the CAD system and records management system (RMS). VMware hosts should be dedicated to the public safety environment. This is a best practice that assists in troubleshooting issues and protects the system from accidental performance-affecting configuration changes by non-public safety information technology (IT) personnel.*

Note: As recommended (Section 4.1.2 vSphere Hosts) within the Assessment Report:

> *Add hosts to provide resources at both the primary and secondary sites to host all public safety servers in the event of a network failure between sites. Disaster recovery will not work without having enough resources at both sites.*

Note: As recommended (Section 4.1.9 Disable DRS[1] for Public Safety Servers) within the Assessment Report:

> *Public safety servers only should be moved between hosts manually. Short-duration outages between sites can cause a "split brain" issue, which was experienced while MCP's SME was onsite. During events that place a high demand on the public safety servers, automatic moves of servers can affect access to the system at times when loss of access can impact first responder safety.*

Phase 2: Network Segmentation/Separation and Redundancy Recommendation

Move the public safety VMWare environment and dispatch workstations to dedicated network equipment and subnet.

- Increased security
- Eliminates outages caused by network load spikes
- Provides failover of links reducing outages

Note: As recommended (Section 4.1.7 Network) within the Assessment Report:

> *Separate the public safety network from the rest of the County's network. This will increase the security of the public safety network and prevent performance issues caused by traffic on*

[1] Distributed resource scheduler

the rest of the County's network. Doing so also will protect the network from accidental performance-affecting configuration changes by non-public safety IT personnel.

Note: As recommended (Section 4.1.15 Network Redundancy) within the Assessment Report:

Increase the number of switches and switch ports to provide enough ports in case of a switch failure. Redundant links between sites that are dedicated to public safety traffic provide for failover and limits traffic to required traffic.

Add Internet Connection

Add additional internet connect from a different carrier and move all remote CAD users to the new connection. The current internet connection will be used for failover in the event of an outage:

- Increased security
- Dedicated bandwidth to public safety
- Eliminates outages and delays caused by internet usage
- Provides failover

Note: As recommended (Section 4.1.3 Internet Link) within the Assessment Report:

Add a second internet connection from another internet service provider (ISP) to provide for failover and redundancy. The internet connections should be geographically separated and be used in an active-active configuration to reduce internal network traffic by directing traffic to the closest link.

Note: As recommended (Section 4.1.8 Dedicated Internet Connections) within the Assessment Report:

Add a dedicated internet connection for public safety and NetMotion Software clients. All County traffic is using one internet connection, which has caused remote-user connection issues due to the high utilization of this link. This also provides better security and access control regarding the public safety systems.

Scope of Work

Phase 1: VMWare Environment Replacement Remediation

Based on conversations with Fulton County that the current VMWare environment hosting the Public Safety servers cannot be dedicated to them, Mission Critical Partners is recommending a new VMWare environment for the public safety servers.

The cutover to new VMWare hardware will not impact clients because we will use Neverfail to move the servers. During Phase 2, there will be a planned outage as the site-to-site virtual private networks (VPNs) are switched to the new firewall and internet connections.

On the following pages, MCP has outlined our approach and solution for Fulton County to complete the recommendations given in the assessment. We plan to divide the effort into five distinct tasks.

Phase 2: VMWare Environment Replacement Remediation		
Task #	**Description**	**Tasks**
1.1	Kickoff Meeting	• Coordinate with the County's IT staff to answer questions and provide technical support.
1.2	On-site Installation of VMWare	• Install and configure VMware environment
1.3	Remote VMware Configuration	• Created virtual servers as needed • Configure storage as needed • Migrate existing virtual server from the old cluster
1.4	On-Site Cutover	• Verify all service has been configured properly for the new environment • Work with Fulton County and Central Square to cut over to the new system
1.5	Documentation	• Provide as-built diagrams and documentation

In the sections that follow, MCP provides a comprehensive analysis of our approach during each phase of the project.

Task 1.1: Kickoff Meeting

MCP will conduct a project kickoff meeting with the project team and stakeholder representatives to:

- Establish mutual acquaintance
- Clarify roles
- Coordinate timing and action items between County resources and MCP

MCP's service program manager will facilitate the meeting. Prior to the meeting, MCP will review available documentation regarding:

- VMware virtual environment
- Storage environment

Kickoff Meeting Review

Project and task milestones
Schedules and deliverables
Project budget
System technology

At the conclusion of the kickoff meeting, the County and MCP will be aligned on the schedule and tasks required to complete this project.

Task 1.2: On-Site Initial Configuration of System

The MCP program manager will be responsible for the initial configuration of the system hardware. The following steps will be taken by the program manager to complete this phase:

- Initial configuration of the storage-area network (SAN)
  - Internet Protocol (IP) addressing of all ports

  - Controller parameters
  - Initial Storage Configuration
  - Internet Small Computer Systems Interface (iSCSI) configuration

- Initial configuration of VMware
  - Installation of VMware ESXi software on servers
  - Configuration of ESXi software
  - Adding ESXi to existing VMware vCenter management system
  - Attaching ESXi servers to storage
  - Create required server templates for server provisioning

Task 1.3: Remote VMware Configuration

The MCP program manager will be responsible for the remaining configuration tasks. The following steps will be taken by the program manager to complete this phase:

- Configuration of VMware datastores on SAN
- Provisioning of required virtual servers
- Migrating existing virtual servers from an existing VMware cluster as needed
- Update site documentation to reflect new hardware

Task 1.4: On-Site Cutover

The MCP program manager will be responsible for the cutover of all current CAD servers to the new VMware cluster. The following steps will be taken by the program manager to complete this phase:

- Verify all service has been configured properly to support the CAD applications
- Work with Fulton County and CentralSquare staff to cut over to the new hardware.
- Install metal fencing with a gate in the public safety answering point (PSAP) data center

Task12.5: Documentation

The MCP program manager will be responsible for providing “as-built” documentation.

- Configuration of the VMware environment
- Provisioning of virtual servers
- Network diagram

Phase 2: Network Segmentation and Redundancy Remediation

Task 2.1: Network Redundancy

MCP recommends an increase in the number of switches to provide enough ports in case of a switch failure. In the event of a switch failure, cables from the failed device can be moved to the spare ports on the other. In addition, redundant links dedicated to the public safety traffic between sites should be implemented to provide for failover and enhanced management of traffic.

Task 2.2: Enhanced Internet Connection

Add additional internet connection from a different carrier and move all remote CAD user traffic to the new connection. The current internet connection will be used for failover in the event of an outage. The internet connection should be protected by dual firewall security appliances configured in a failover cluster.

- Advantages:
  - Increased security
  - Dedicated bandwidth to public safety
  - Eliminates outages and delays caused by non-public safety internet usage
  - Provides failover and redundancy

Task 2.3: Network Time Protocol

Install two new Network Time Protocol (NTP) servers. One to replace the current end-of-life server and one for failover.

- Advantages:
  - Removes single point of failure
  - Removes “end of life” hardware from network
  - Provides failover
  - Prevents time shift of critical systems due to loss of time reference
  - Ensures all public safety systems have common time references.

Proposed Staff

MCP recognizes that as an independent solutions provider, our corporate capabilities depend directly on the capabilities and experience of our staff. MCP has assembled one of the most experienced and knowledgeable teams in the country. A multifaceted project such as this requires different areas of expertise and knowledge—typically more than any one or two individuals can bring—because different areas of expertise often are required at different stages of the project.

Chris Faircloth, Business Development Manager

Client Services Manager

Chris Faircloth brings extensive 911 and telecommunication industry expertise to state and local government agencies to support the public safety community. His background encompasses all facets of 911 and next-generation technical and operational standards, as well as a wide range of technological solutions and experience that includes land mobile radio (LMR) and CAD systems. His work involves the development, procurement, and implementation of many multi-million-dollar public safety projects. Through his work on public safety projects, Chris brings a solid understanding of procurement and contract development within the state and local government landscape. He brings extensive experience in understanding and representing customers to make sure that services are pertinent to solving their exact needs.

Mark Moloney, MCSE, CCNP, IT Network Manager

Service Program Manager

Mark Moloney is a Microsoft Certified Systems Engineer (MCSE), Cisco Certified Network Professional (CCNP), GIAC Security Essentials (GSEC), GIAC Certified Windows Security Administrator (GCWN) with more than 20 years of extensive network technical experience in the IT field, emphasizing network administration, security management, and server support. He is an excellent problem solver with strong communication and interpersonal skills. Mark is a former military professional that is successful at building strategic partnerships and alliances and spearheading business relationships to achieve beneficial outcomes.

Patrick W. McFeely

Enterprise Client Manager

Pat is a public safety communications subject matter expert who has been engaged in the management and oversight of communications projects for more than 30 years. He provides clients with technical expertise in areas related to the planning, design and integration of EOC facilities, radio systems, alert warning systems, enhanced grounding systems, and A/V systems. Currently, Pat provides executive- and technical-level services for the Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA) Chemical Stockpile Emergency Preparedness Program (CSEPP) and multiple other State and Local agencies.

Jim Krebs

Senior Technology Specialist

Jim is a Senior Technology Specialist with more than 30 years of facilities and mechanical, electrical experience. He is certified and specializes in Motorola R56 standards and compliance to ensure the client's communication systems achieve maximum longevity, reliability and optimal level of performance. Jim has supported initiatives to hold contractors accountable and guarantee R56 grounding compliance in the construction of new communication and PSAP facilities to ensure client quality and safety. Jim has provided R56 support to DHS/FEMA CSEPP in Kentucky for Madison County and Lexington, Kentucky and recently performed and completed an R56 compliance audit for MOSWIN systemwide testing.

Mike Beagles, Platform and Service Product Manager

Technical Lead, Network Infrastructure Update

Mike Beagles, Senior Technology Specialist, has been working in the IT field for more than 15 years, with 10 years specifically supporting public safety environments. During that time, Mike has designed and implemented a long list of technologies that support the public safety mission. He was the chief architect and implementer of EmergiTech's InterCAD system delivered over the network as a service to 911 agencies around the country. As an IT manager, he served as a technical lead on CAD, records management system (RMS), 911 and mobile projects. Mike has expertise in networking and network design, security and accessibility, server design, and application delivery. Mike attended Houston Community College, C-TREC Technical School Cisco Certified Network Associate (CCNA) Bootcamp, and holds certifications with Microsoft Server and Comp Telecommunications Industry Association (TIA).

Kevin Bresnahan, VP & Director of Lifecycle Management Services Delivery Operations

Client Manager

Kevin Bresnahan has more than 30 years of extensive experience in customer advocacy, systems operation, network operations center (NOC) monitoring operations, security services operations, technical support and field service operations gained throughout a long term career with a number of large technology companies, some within the public safety sector. Kevin earned his Bachelor of Science Degree from Salem State University, Salem, Massachusetts, and his Master of Business Administration (MBA) from the University of Colorado.

David S. Jones, President, Lifecycle Management Services Division

Customer Advocacy and Quality Assurance

David S. Jones will provide the customer advocacy and quality assurance (QA) overview and review of all deliverables and provide additional project management support to the project and client managers as needed. David's background includes more than 30 years of operations management, services management, strategic and tactical planning, vendor management and contract management within the public safety sector for a large technology company and a couple of smaller companies. David directly managed more than 1,600 people and 900 contract partners and completed on-time projects with an average annual value greater than $500 million per year during his prior tenure with the large technology company. He also owned more than $250 million in contracts for technology maintenance, support and management. David earned his Bachelor of Science degree in engineering and an MBA degree in Systems Management.

Pricing

Fulton County agrees to purchase Phase 2: VMWare Environment Replacement Remediation services as described in the scope of work for the **total fee of $64,000**, including expenses. Phase 3 Network Segmentation and Redundancy Remediation services as described in the scope of work will be provided for the **total fee of $98,000**. Phase 2 and Phase 3 Remediation services total fee is **$162,000,** of which a PO 22020SC123328B-JD has been issued previously for $156,400, services not yet rendered.

Hardware is scoped, and a quote is provided that utilize Stratus components which provide fully fault-tolerant servers for a **total hardware fee of $560,455**. Details on the bill of materials can be found in Appendix D.

MCP will invoice Fulton County on a monthly basis on a percent complete basis of all recommended actions. Payment terms are proposed to be net 30 days upon the receipt of an invoice by Fulton County.

Table 1: Pricing Summary – Stratus Components

Description of Service	Fee
Phase 2 and 3	
Phase 1: VMWare Environment Replacement Remediation	$64,000
Phase 2: Network Segmentation and Redundancy Remediation	$98,000
Phase 1 and 2 Sub Total	$162,000
Hardware	
Hardware Stratus (Appendix D)	$560,455
Additional Items	
Comcast Connection (Appendix E)	$62,500
Central Square Consulting (Appendix F)	$99,450
Total	
Sub Total	$884,405
Purchase Order 22020SC123328B-JD	($156,400)
Total	$728,005
Maintenance and Support year 1*	0
Maintenance and Support year 2	$132,078
Maintenance and Support year 3	$132,078
Maintenance and Support year 4	$144,828
Maintenance and Support year 5 +	$144,828

Assumptions

- Fulton County, Georgia will be responsible, if necessary, for any updates to PSAP data center UPS and or generator functionality
- The County's current DR site hardware will be used to support the Public Safety servers
- The Central Square software package and maintenance are directly contracted through the county and are not associated with this proposal

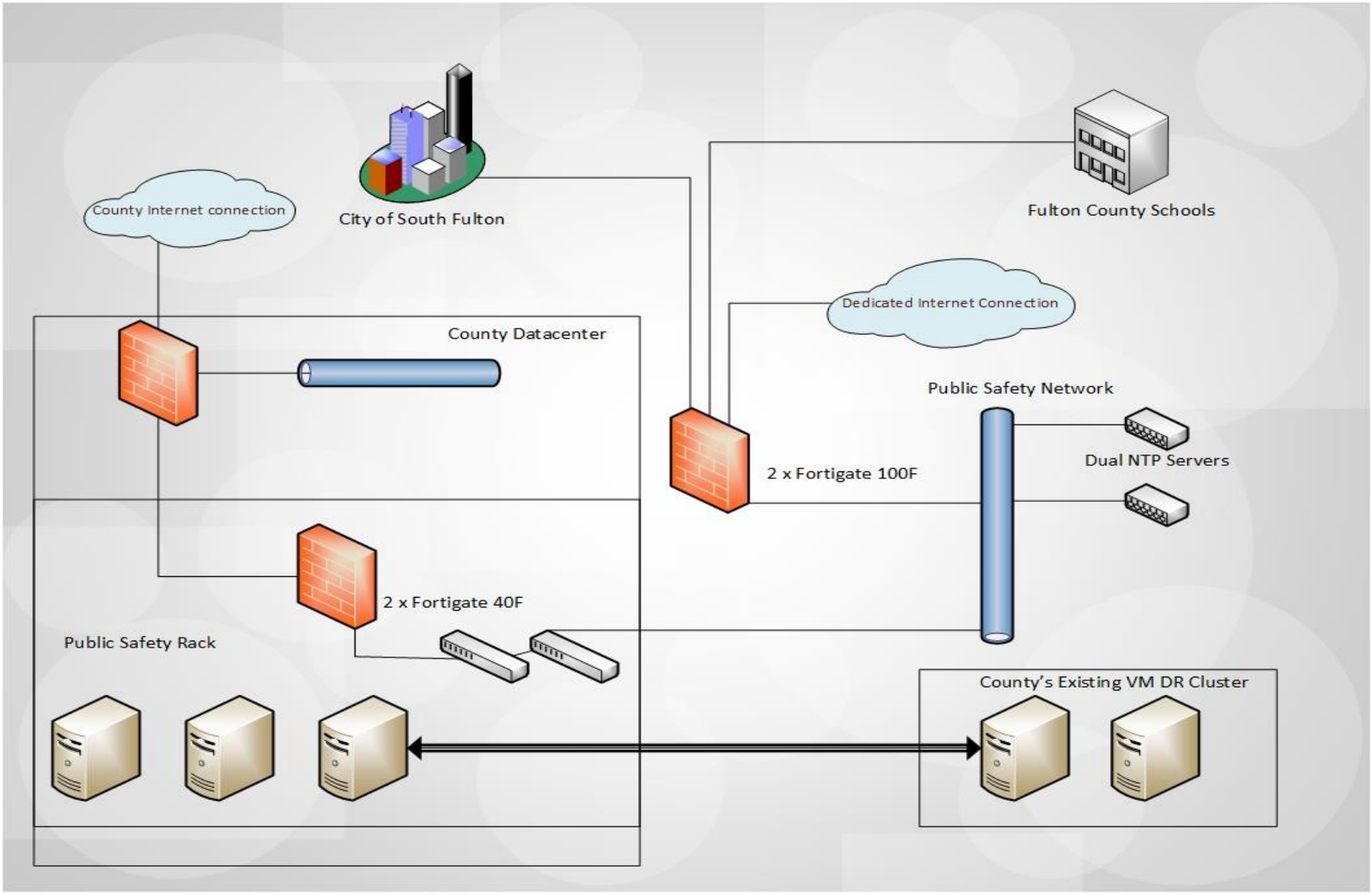
Signature Page

MCP is prepared to move ahead with the additional support upon notification to proceed via purchase order or signature below. We will schedule our support implementation promptly upon notification.

Agreed To and Accepted

Fulton County, Georgia	Mission Critical Partners, LLC
Name:	Name: David S Jones
Title:	Title: President LMS Division
Date:	Date: December 29, 2021

Appendix A: Phase Three Recommendations Diagram



Appendix B: Hardware Requirements

Item Pricing			
Quantity	**Product Code**	**Product**	**Product Description**
3.00	HEP-DL380G10-Fulton	HPE DL380 Gen10 Server	• DL360 GEN10 4210R 1P 16G NC 8SFF SERVER • QTY 2 CPU = DL380 GEN10 XEON-S 4214R KIT • 256GB RAM - 32GB 2RX4 PC4-2933Y-R SMART KIT • QTY 2 - 600GB SAS 15K SFF SC DS HD • ILO ADV INCL 3YR TS U E-LTU • 500W FLEX SLOT PLAT HPLUG LH P/S KIT • SN1100Q 16GB 1P FC HBA • VMW VSPHERE STD 1P 5YR E-LTU • CAREPACK 5YR FC 24X7 DL360 GEN10 SVC • CAREPACK 5YR 24X7 ILO ADVPACK NON BL 3YR • CARE PACK INSTALL/STARTUP DL380 G4 G5 DL
1.00	HPE-MSA2060-Fulton	HPE MSA2060 Storage	• MSA 2060 16GB FC SFF STOR • QTY 2 - 4PK MSA 16GB SW FC SFP XCVR • MSA 5.4TB 15K SFF M2 6PK TAA HD BDL • 5YR FC 24X7 MSA 2060 STOR SVC • CARE PACK INSTALL/STARTUP MSA2060
1.00	NSX42UKIT-UPS	DELL EMC Rack Kit	• Dell Netshelter SX 42U Rack - 600mm Wide x 1070mm Deep • (2) AP 7540 – Basic PDU 208V 0U RM 20xC13 4xC19 NEMA L6-20P • 17-inch Rack LCD Console with Integrated 8 Port Analog KVM Switch • (8)APC INTEGRATED LCD KVM USB CABLE - 6 FT 1.8M • APC Smart-UPS SRT 5000VA RM - UPS - 4250-watt - 5000 VA - with 208V to 120VStep-Down Transformer • APC Smart-UPS SRT 192V 5kVA and 6kVA RM Battery Pack - battery enclosure lead acid • Installation Services for APC NetShelter Rack
2	FG-40F-BDL-950-12	Fortinet 40F	• Hardware plus 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)

Item Pricing			
Quantity	**Product Code**	**Product**	**Product Description**
2	FG-100F-BDL-950-12	Fortinet 100F	• Hardware plus 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)
2.00	C9300-48T	Cisco C9300-48T	• CATALYST 9300 48PORT DATA ONLY PERP NTWK ADVANTAGE • 350W AC 80+ PLAT CONFIG 1 PWR SECONDARY PWR SUP • PLUGGABLE USB 3.0 SSD STORAGE INT50CM TYPE 1 STACKING CABLE CABL • CATALYST STACK PWR CABL 30CM CABL • CCW ONLY SOLN SUP SW SUB C9300 SVCS 48PORT DNA PREMIER • 3YR TERM LICS C9300 DNA PREMIERLICS 48PORT • CCW ONLY SOLN SUP SW SUB SVCS CATALYST DNA PREMIER • 3YR DNA PREMIER CATALYST ADD-ONLICS TERM LICS • CATALYST 9300 8X10GE NETWORK CPNT MODULE PER CISCO DIR SHIP ONLY • 7/20 • CCW ONLY SOLN SUP 24X7 4HR OS SVCS CATALYST 9300 48PORT DATA ONLY NTWK
2.00	NKS-C9318YC-EX	Cisco NKS-C9318YC-EX	• NEXUS 9300 WITH 48P 10/25G SFP+PERP AND 6P 100G QSFP28 • QTY 24 - 1000BASE-T SFP TRANSCEIVER MOD PERP FOR CATEGORY 5 • COPPER WIRE • QTY 8 - 10GBASE-CU SFP+ CABLE 3M PERP • QTY 4 - 10GBASE-LR SFP MODULE PERP • 3YR ONE ADVANTAGE TERM N9300 XFLICS • CCW ONLY 24X7X4 SNTC NEXUS 9300SVCS WITH 48P

Item Pricing			
Quantity	**Product Code**	**Product**	**Product Description**
2.00	9438PKG	NetClock Time Server Package	• NetClock Time Server 9483 • OCXO (1U) Option for GPS Backup • Netclock 9483 Gigabit Ethernet Card • GNSS Outdoor Antenna • GPS Antenna Surge Protector • Post Mounting Kit • Grounding Kit • Low Loss Antenna Cable • Premium Support Package • 4 Inch Green 6-digit IP Clock POE • 110-220V 50-60Hz Power Injector
12.00	NESWS1UPGRADE	Neverfail Enterprise Support with WAN Smart UPGRADE - 1 pack	• Upgrade one basic license pair to include WAN Smart
12.00	NF-INSTALL	Neverfail Installation Services	• Installation services for Neverfail Software. Remote services only.
1.00	ProServ Tier2	NEWCOM Services Tier 2	• NEWCOM Services - Tier 2: • The hardware or software purchased comes with the manufacturer's warranty and technical support as described in our Tier 1 offerings. This product allows the customer an out-of-the-box setup experience to solve the problem they are facing. In addition to additional setup, configuration, post-service support by phone or email, and extended warranties are included. • Please note, the following option is available from NEWCOM with your purchase at an additional cost: • Tier 3: The hardware or software purchased comes with benefits noted in Tier 1 and Tier 2, along with extended warranties beyond what is available by the manufacturer. The NEWCOM team will install, support, and keep an inventory of critical infrastructure and replacements. • Tier 2 Services are renewed annually.

Appendix C: COMCAST Requirements

Comcast Confidential Page 1 10/6/2021

Enterprise Business Services
Proposal
For
Mission Critical Partners (MCP)
Submitted by:
Nikita Johnson
Strategic Enterprise Account Executive
October 6th, 2021
CONFIDENTIAL Comcast Confidential Page 3 10/6/2021

Enterprise Ethernet Dedicated Internet Service Options

Proposed Services				
Service Type	**Anticipated Turn Up Date**	**Installation Charges**	**Monthly Recurring Payment**	**Term**
5G ETHERNET DEDICATED INTERNET	30-90 Days	NONE	$4,200.00	36 Months

Appendix D: Central Square Consulting

CENTRALSQUARE

Quote prepared on:
October 21, 2021
Quote prepared by:
Sara Nusbaum
sara.nusbaum@centralsquare.com

Quote #: Q-64805
Primary Quoted Solution: ONESolution PS
Quote expires on: November 30, 2021

Quote prepared for:
Mark Maloney
Mission Critical Partners
130 Peachtree Street, SW
Atlanta, GA 30303

Thank you for your interest in CentralSquare. CentralSquare provides software that powers over 8,000 communities. More about our products can be found at www.centralsquare.com.

WHAT SERVICES ARE INCLUDED?

DESCRIPTION	TOTAL
Public Safety Project Management Services - Fixed Fee	13,260.00
Public Safety Technical Services - Fixed Fee	66,300.00
Services Total	79,560.00 USD

QUOTE SUMMARY

Services Subtotal	79,560.00 USD
Quote Total	**79,560.00 USD**

WHAT ARE THE RECURRING FEES?

TYPE	AMOUNT
FIRST YEAR MAINTENANCE TOTAL	0.00

MORE INFORMATION AT CENTRALSQUARE.COM

Appendix F: Maintenance Costs

Item	Service duration (months	Amount per renewa	Item Quantity	Maintenance Amount		year 1 maintenance cost	year 2 maintenance cost	year 3 maintenance cost	year 4 maintenance cost	year 5 maintenance cost
Stratus Maintenance and Support	12	$ 16,990.68	1	$16,990.68		$ -	$ 16,990.68	$ 16,990.68	$ 16,990.68	$ 16,990.68
Fortinet	12	$ 6,209.35	4	$24,837.40		$ -	$ 24,837.40	$ 24,837.40	$ 24,837.40	$ 24,837.40
NEWCOM Tier 2	12	$ 39,550.00	1	$39,550.00		$ -	$ 39,550.00	$ 39,550.00	$ 39,550.00	$ 39,550.00
12-month Subtotal				$81,378.08		$ -	$ 81,378.08	$ 81,378.08	$ 81,378.08	$ 81,378.08
Cisco Catalyst 9300	36	$ 8,683.65	2	$17,367.30		$ -	$ -	$ -	$ 5,789.10	$ 5,789.10
Cisco Nexus	36	$ 10,441.20	2	$20,882.40		$ -	$ -	$ -	$ 6,960.80	$ 6,960.80
36-month Subtotal				$38,249.70		$ -	$ -	$ -	$ 12,749.90	$ 12,749.90
Comcast Internet	12	$ 56,952.00	1	$50,400.00		$ -	$ 50,400.00	$ 50,400.00	$ 50,400.00	$ 50,400.00
Comcast IP addresses	12	$ 339.00	1	$300.00		$ -	$ 300.00	$ 300.00	$ 300.00	$ 50,400.00
12-month Subtotal				$50,700.00		$ -	$ 50,700.00	$ 50,700.00	$ 50,700.00	$ 50,700.00
* Support costs may increase as manufacturers adjust their costs in the future.					TOTAL	$ -	$ 132,078.08	$ 132,078.08	$ 144,827.98	$ 144,827.98
* Neverfail Annual costs will still be handled directly by NEWCOM, as they are currently.										
*-Year 1 Maintenance start upon delivery of the HW										