The parties to this service agreement agree to the above referenced conditions:

FULTON COUNTY, GEORGIA

Robert L. Pitts, Chairman
Fulton County Board of Commissioners

Tonya R. Grier, (SEAL)
Interim Clerk to Board of Commissioners

Approved as to Content:

Glenn Melendez, Interim CIO
Information Technology Department

Approved as to Form:

Office of the County Attorney

MISSION CRITICAL PARTNERS, LLC

(Submitted By)

(Approved By) Authorized Representative

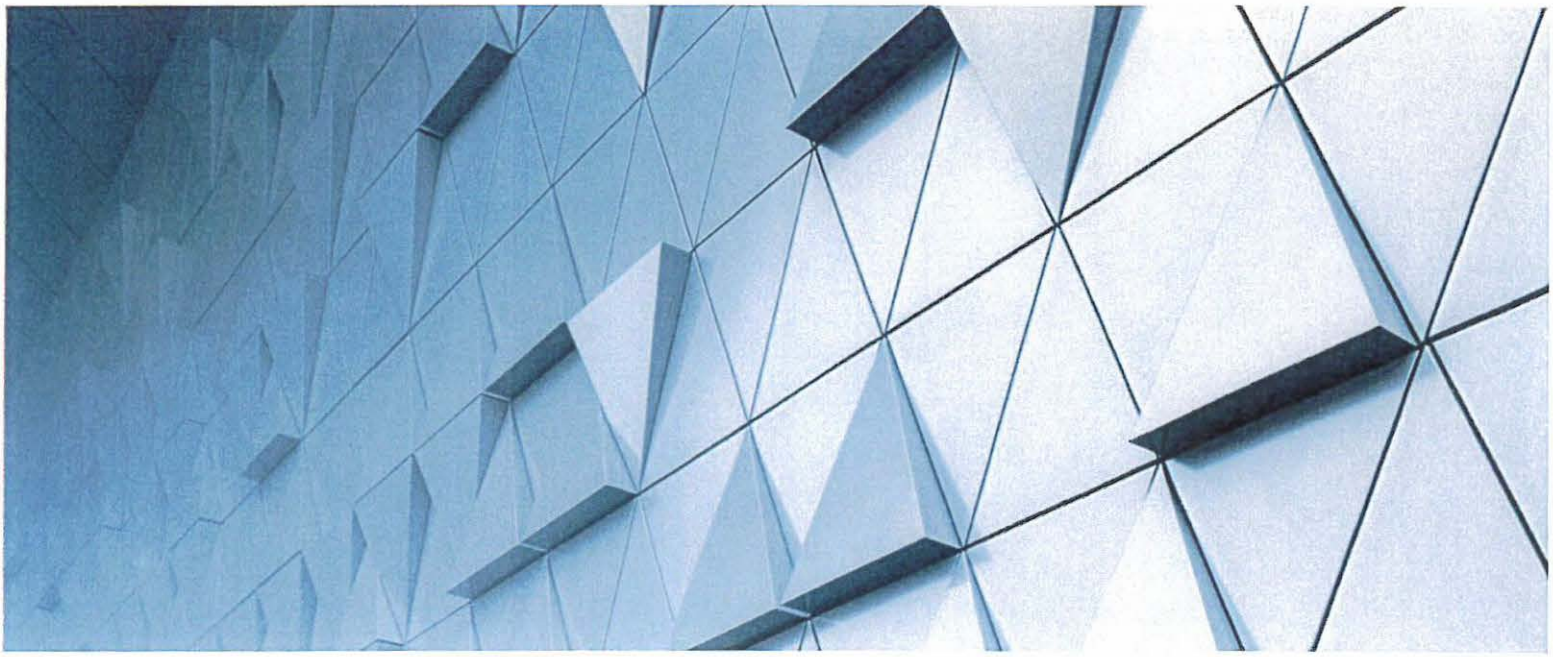
Vice President, Director of Administrative Services

(Title)

Date: 1 / 17 / 2020

ITEM # 19-1132 RCS 12/18/19
RECESS MEETING

ATTACHMENT A



MissionCriticalPartners
Because the Mission Matters

Computer-Aided Dispatch Performance Remediation and Support Services

NetPulse Scope of Work

PREPARED JANUARY 9, 2020 FOR
FULTON COUNTY, GEORGIA

MissionCriticalPartners.com
State College Office | 690 Gray's Woods Blvd. | Port Matilda, PA 16870 | 888.8.MCP.911 or 888.862.7911

Scope of Work

Phase 1: Mission-Critical NetPulse℠ Advanced (Network & Application Monitoring and Support)

Monitoring

All network links, firewalls, and servers should be monitored for performance and uptime/downtime. The monitoring should provide notifications and trending to assist in proactive network support before issues affect users' experience or cause system outages. This also facilitates planning for growth and troubleshooting issues.

Mission-Critical NetPulse℠ Essential

The proposed **NetPulse Essential** network support service provides Fulton County (County) with a view into its network and enables the County to monitor and support its network's compliance with the Information Technology Infrastructure Library (ITIL) service operation standard. An exclusive and secure environment specific to the County is established within MCP's integrated services platform. All networking devices are discovered and established within the platform's database. This populates the platform's real-time device and circuit health dashboard, enabling the client to have 24 hours a day, seven days a week (24x7) view of device and network performance and alerts. A monitoring profile is deployed to all devices, establishing performance thresholds for alerting. Notification rules are enabled, providing a means for network support personnel to be notified when a device or circuit experiences a failure. Ticketing also is enabled, enabling the County to track all incidents to resolution and track historical patterns of issues and failures. All performance, bandwidth utilization, and fault data are stored in the database, enabling reporting capability with a robust set of data.

Task 1.1: Establish the Network Management Environment

MCP will establish an exclusive and secure network management environment specific to the County. Specifically, MCP will:

1. Establish the environment for the County to facilitate network monitoring, ticketing, and device management.
   a. MCP will configure the environment as required per the definitions defined below.

2. Provide secure access to the County's network management environment for up to four individuals.

3. Provide the County with up to 20 hours of orientation and training for the network management platform, for up to four individuals.

Task 1.2: Configure the Network Management Environment

1. To specifically define the devices to be monitored, MCP will review the proposed monitoring inventory with the County and will make changes at the County's request.

2. To specifically define what processes and elements within a specific device will be monitored, MCP will review the proposed monitoring templates with the County and will make changes at the County's request.

3. To understand the handling procedures for any potential monitoring alarm, MCP will review with the County the proposed support process and will make changes at the County's request.

4. MCP will create a customer support plan specific to the delivery of the network monitoring service to the County. This document will be used as the ongoing delivery document, and will include:
   a. All relevant contact information
   b. Escalation matrices
   c. Notification definitions
   d. Support process flow steps and definition, including planned maintenance process
   e. Monitoring device inventory
   f. Monitoring templates

Task 1.3: Prepare the Network for Monitoring and Test through Burn-In Period

1. MCP will discover items within the management platform as needed for monitoring via Simple Network Management Protocol (SNMP) enabled by the County.

2. As needed, MCP will require Secure Socket Shell (SSH) log in credentials working with the County for this effort.

3. MCP will work with and guide the County regarding how to deploy management agents on all devices as needed for monitoring said devices via a device agent.

4. MCP will test that all devices defined within the network monitoring inventory are connected and are reporting appropriately.

5. MCP will test that all notifications are functioning as agreed to by the County.

6. MCP will test that all actions defined within the monitoring template (e.g., auto-ticketing, notifications) are functioning as defined.

7. MCP will test that all network management platform views extended to the County are working properly.

8. MCP will confirm that report availability is functioning properly.

9. MCP will provide functional reviews on a biweekly basis, via conference calls, with the County through the initial 30-day burn-in period.

Task 1.4: Ongoing Support of Network Monitoring

1. MCP will provide functional reviews monthly, via conference calls, with the County throughout the life of the agreement.

2. MCP will provide support by phone and up to six on-site visits upon request for issues specific to the monitoring service throughout the life of the agreement.

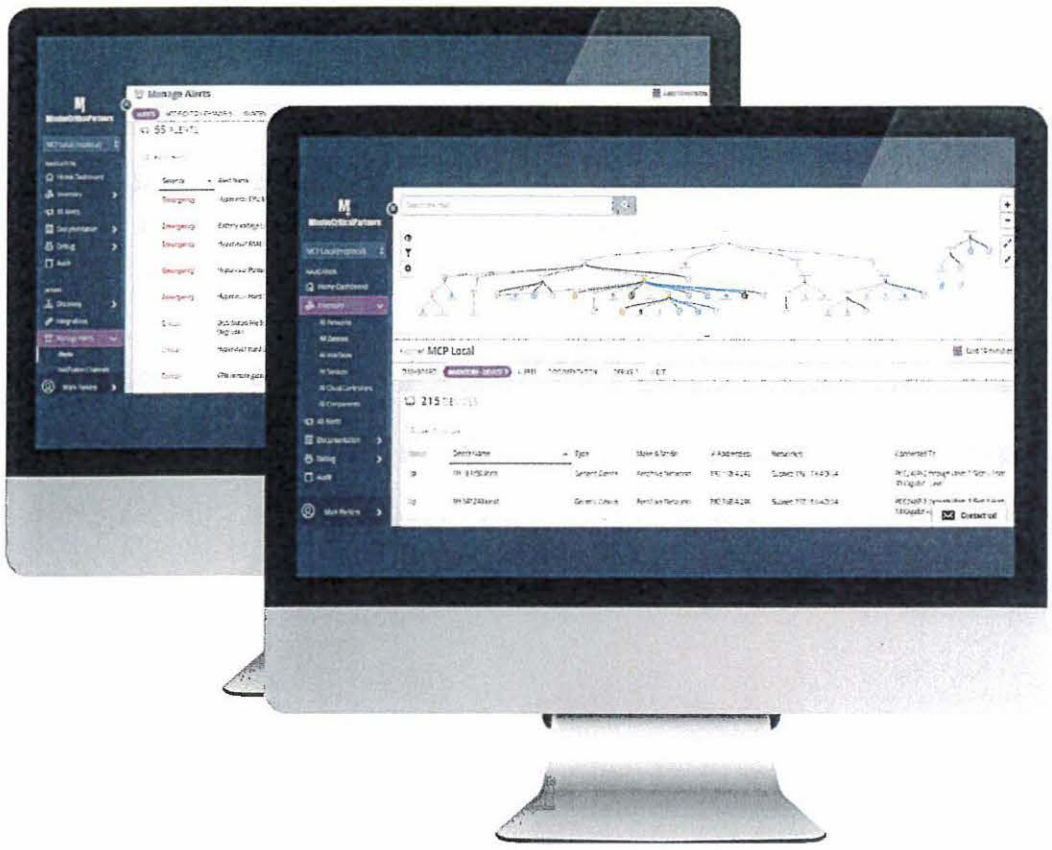


Figure 1: NetPulse Essential

Mission-Critical NetPulse[SM] Advanced Monitoring Services

NetPulse Advanced monitoring services provide proactive and highly responsive around-the-clock remote support services via a network operations center (NOC) that mitigates, escalates, responds and resolves network incidents quickly. Our field engineers and specialists develop a deep understanding of the client's network environment and coordinate with every key network component provider and vendor involved with the network on behalf of the client, acting as a clearinghouse that manages incidents and events until issue resolution.

The NetPulse Advance program includes a comprehensive set of services:

- Establish a secure connection between the agency system and the MCP NOC
- Maintain User Guide – including contact information and help desk instructions
- Provide a help desk to answer your questions, provide advice and solve problems
- Dynamically collect status information
- Set thresholds for alerts
- Monitor the status of systems and network (see below for details)
- Respond when something needs attention
- Analyze and report on conditions – provide monthly reports on routine matters and immediate reports on critical conditions
- Provide recommendations to keep systems and networks functioning properly

- Assist with the operating system and application updates
- Serve as an advocate for the agency when dealing with multiple support providers
- Deploy staff when on-site services are needed

Systems and Network Monitoring

NetPulse Advanced monitoring utilizes a server to collect and transmit data to the MCP NOC services team. The following are representative of the conditions monitored:

Server Monitoring
- Virtual environments
- Processor and memory utilization
- Disk utilization
- Services
- Print queues
- Error reports
- Event logs
- Time sync
- Backup logs
- Logs for high availability disk arrays

Network Monitoring
- Device status (up/down)
- Average response time (ping) to device
- Packet loss to device
- Processor utilization
- Memory utilization
- Port utilization

In summary, MCP monitors the environment and engages as soon as a detected issue requires attention.

Problem Resolution

As issues are identified, MCP follows a triage model, working along with your staff, to isolate the matter into one or more of the following categories:
- Application
- Hardware
  - Server
  - Storage
  - Computer-aided dispatch (CAD) Workstation
- Database
- Virtualization
- Network
- Remote systems and interfaces (not being monitored)

Once the issue is assessed, MCP will either resolve the issue or engage your staff and the other parties involved. MCP will monitor the status until the matter has been resolved.

Communication's and Reporting

Critical issues and conditions are communicated to the agency immediately. Any other monitoring results will be reported monthly at a minimum. The monthly reports include:

- All detected issues
- Corrective actions taken
- Summary of tickets created
- Review of system performance and utilization
- Link to a customized dashboard
- Required site actions

In addition to these communications, MCP assists in organizing monthly status calls that are attended by a wide range of stakeholders including representatives of management, the primary users within the agency, the applications provider, IT support personnel and others.

Help Desk

NetPulse Advanced monitoring includes a comprehensive telephone support desk that is available for reporting issues, requesting services, solving routine matters and answering questions during normal working hours.

The help desk and support are available 24x7x365 for critical matters.

Prerequisites

The success of NetPulse Advanced is based upon the condition and capacity of the environment to support the requirements of the application systems. It is also based upon MCP engineers having an in-depth understanding of the requirements and the environment.

MCP will utilize the results of the recent CAD services assessment to establishing the NetPulse Advance service:

Agency Support and Facilities

The following are needed for MCP to monitor and perform troubleshooting triage of the systems and network:

- Remote access to the site using a virtual private network (VPN) or another secure access facility
- A server to support monitoring – can be a virtual machine
- Ability to send email alerts and reports from the monitoring system to MCP
- Agency contact to assist in coordinating support services
- Onsite assistance during triage and other problem-solving activities

Service Level Agreements

Service level agreements for the NetPulse Advanced monitoring are as follows:

- Coverage is 24 hours per day, 7 days a week, 365 days per year

- Response to alarm or phone call to service desk is 98% of all alerts/calls will be responded to in less than 15 minutes.
- Engagement for resolution for high severity incidents, as agreed to by the county, is immediate and continuous until resolution. For low severity incidents, as agreed to by the county, is next business day.

Phase 2: On-site CAD Network Support Engineer

In this phase, MCP proposes an on-site CAD Network/Hardware support engineer. The resource will be an MCP employee, dedicated full-time to the Fulton County project and in support of the business interests of Fulton County. MCP will be responsible for all employment salary, benefits, taxes and management of this resource.

The dedicated MCP Network Support Engineer will work a standard work week of 40 hours, with the MCP benefit of 17 days PTO and 7 paid holidays. The Support Engineer will be the primary face to the County in the management of outages and incidents on a 24 by 7 basis, but will also have the 24 x 7 support of the Mission Critical Partners services organization. Should the dedicated Support Engineer not be available due to illness or PTO, support will be provided by the MCP services organization. The primary work location for the dedicated Support Engineer will be a work space on site as assigned and provided by Fulton County. The dedicated Support Engineer will provide the County a monthly status report of all incident activity, and other specific tasks and effort performed.

Responsibilities of the Network Support Engineer will include, but are not limited to:

- Incident response
- Vendor focal point for county
- Assist in remediation actions
- Root cause analysis
- Coordinate and facilitate monthly status meetings
- Make additional proactive recommendations to improve security and reliability
- Execute the application of operating system updates, required configuration changes, and other required patches and updates.
    - All updates will be managed per a defined change control process requiring agreement by the County regarding the details, update process, and timing of the specific change. Every effort will be made to leverage Neverfail functionality to ensure that application operation is not interrupted.

Phase 3: Program Management and Remediation Services

Virtual Machine Ware Environment Replacement

Based on conversations with Fulton County that the current virtual machine ware (VMW) are environment hosting the Public Safety servers cannot be dedicated to them, MCP 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 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 phases.

Task #	Description	Tasks
1	Kickoff meeting	• As part of a remote kick-off meeting, MCP will provide the recommended hardware bill of materials that is compatible with the current environment • Coordinate with the County's IT staff to answer questions and provide technical support.
2	On-Site Installation and Initial Configuration of System	• The MCP program manager will be responsible for the initial configuration of the system hardware.
3	Remote SAN/VMware Configuration	• Created virtual servers as needed • Configure storage as needed • Migrate existing virtual server from the old cluster
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
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 2.1: 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 Fulton resources and MCP
-

Kickoff Meeting Review

Project and task milestones
Schedules and deliverables
Project budget
System technology

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

-
- VMware virtual environment
- Storage environment
- Bill of materials (BOM) for a new system

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

Deliverable(s):

- Project kickoff meeting

Task 2.2: On-Site Installation and 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:

- Install VMware (ESXi) server hardware in client provided equipment rack
- Install storage area network (SAN) hardware in client provided equipment rack
- Cable and label all system connections
  - Power
  - Internet Small Computer Systems Interface (ISCSI)
  - Local Area Network (LAN)
  - Management
  - Keyboard, video, mouse (KVM)
- Initial configuration of SAN
  - Internet Protocol (IP) addressing of all ports
  - Controller parameters
  - Initial Storage Configuration
  - 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

Deliverable(s):

- Server configuration

Assumptions:

- All hardware and software required to support this project will be provided by Fulton County. This will include:
  - VMware ESXi software for new servers, six central processing unit (CPU) licenses required
  - KVM port for ESXi server, three ports
  - Equipment rack for the installation of hardware, 5U (rack units) required
  - Power for hardware, 8 120/240VAC outlets
  - Network switch port for hardware, 22ea 10GBps and 5ea 1Gbps
  - vCenter to manage the new ESXi servers

Task 2.3: Remote 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 form an existing VMware cluster as needed
- Update site documentation to reflect new SAN

Task 2.4: On-Site Cut-Over

The MCP program manager will be responsible for the cut-over 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 have been configured properly to support the CAD applications
- Work with Fulton County and CentralSquare staff to cut over to the new hardware.

Neverfail Deployment

It is our understanding that the county owns Neverfail licenses, and that the product is installed, yet not configured to become operational. Finalizing the configuration and bringing the functionality online will provide necessary backup support to the application that does not currently exist.

Windows Updates

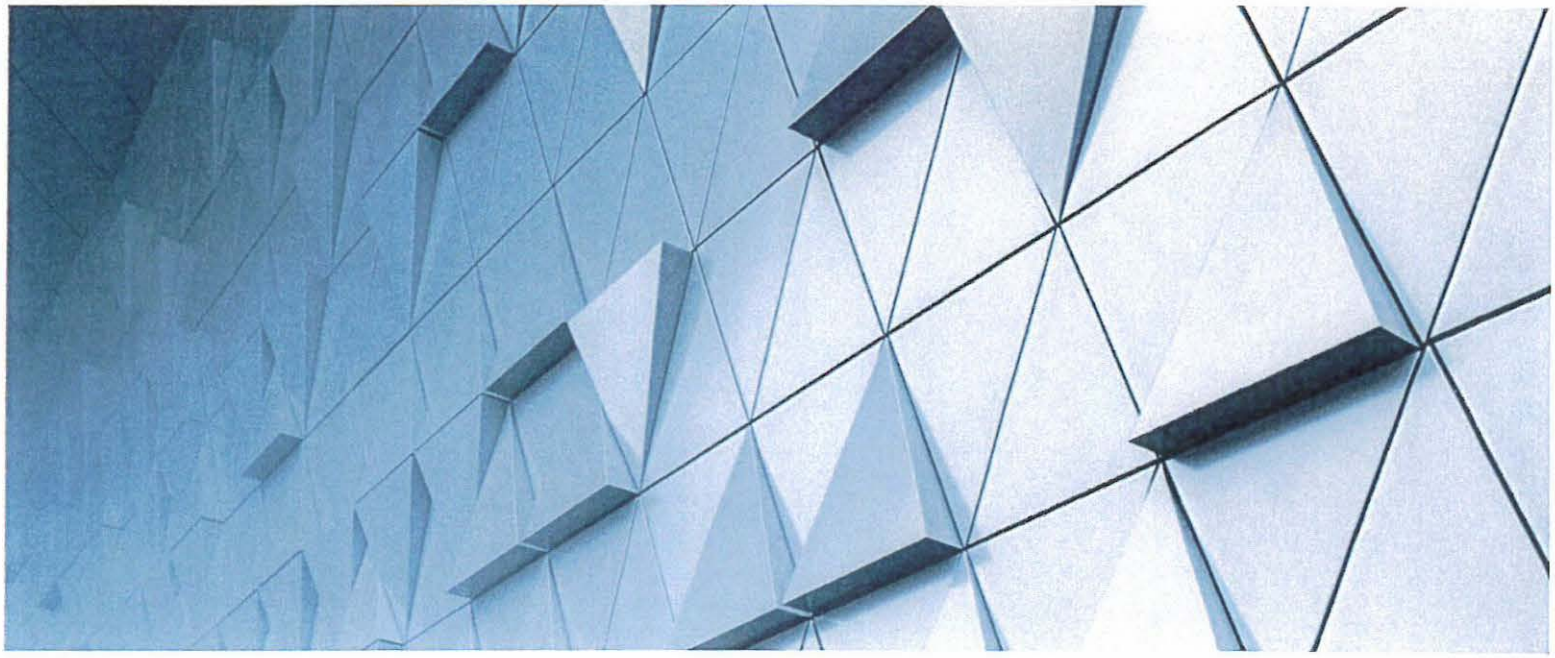
Windows updates should be applied on a regular basis to both workstations and servers after being approved by the IT department and following vendor guidance, and patch levels should be monitored. This protects the system from malware and ensures that all systems are patched to the same level, which eliminates one variable during troubleshooting issues.

Task 2.5: Documentation

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

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

ATTACHMENT B



MissionCriticalPartners
Because the Mission Matters

Computer-Aided Dispatch Performance Remediation and Support Services

Revised Proposal

PREPARED DECEMBER 2, 2019 FOR
FULTON COUNTY, GEORGIA

MissionCriticalPartners.com
State College Office | 690 Gray's Woods Blvd. | Port Matilda, PA 16870 | 888.8.MCP.911 or 888.862.7911

Table of Contents

Introduction Letter

December 2, 2019

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

Re: Proposal for Computer-Aided Dispatch Infrastructure Assessment and Remediations

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 reliability of the system, and greatly improve system and infrastructure support. The foundation of this proposal is the Public Safety Network Assessment performed by MCP the week of September 30, 2019.

Our assessment generated multiple findings and recommendations which we have prioritized into a three-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 Mark Moloney. His contact information follows:

Mark Moloney, IT Network Manager
Mission Critical Partners, LLC
690 Grays Woods Blvd.
Port Matilda, PA 16870

Cell: 321.848.2273
Office: 321.866.8779
Email: MarkMoloney@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

R. Kevin Murray
Chairman & Chief Executive Officer

About Mission Critical Partners

Mission Critical Partners (MCP) is an independent solutions provider that helps public safety clients enhance and evolve their mission critical systems and operations.

Through our breadth and depth of experience and an extensive network of resources, we offer unique, vendor-independent and successful solutions that solve our clients' complex challenges.

Our planning, implementation and information technology (IT) and network support services span all aspects of mission-critical communications, while our expertise covers everything from radio to broadband, networks, and 911, and facilities and operations. We provide confidence and support every step of the way, from design and procurement to building and management. The result is a high-performing emergency response system that achieves maximum value and optimal efficiency.

With MCP, the proof is in the numbers:

- Loyalty is the foundation of our business, with more than 90 percent of our clients remaining with us from project to project.
- Our specialized professionals are integral members of our team, bringing an average of more than 25 years to every project.
- We expand upon our experience year after year, completing more than 700 projects since our inception in 2009.
- We've performed services for clients in nearly all 50 states with a full suite of solutions and services.
- We invest more than a million dollars each year to employee training.

MCP stands behind the importance and nobility of the work our clients do. We understand the criticality of effective and efficient public safety systems, not just for our clients, but for their entire community. While we are proud to have the most experienced and knowledgeable team of professionals in the industry, our greatest pride comes in seeing the successful results of our clients' mission critical operations.

Because at the end of the day, **it's the mission that truly matters.**

OFFICE LOCATIONS

Mission Critical Partners serves municipal, county, state and federal clients across North America with offices in the following locations:

Corporate Headquarters

State College Office
690 Gray's Woods Blvd.
Port Matilda, PA 16870
Phone: 888.862.7911
Fax: 814.217.6807
Web: MissionCriticalPartners.com

Branches

Raleigh Office
3737 Glenwood Ave. Suite 100
Raleigh, NC 27612

Pittsburgh Office
105 Bradford Rd. Suite 400
Wexford, PA 15090

Harrisburg Office
2578 Interstate Dr. Suite 106
Harrisburg, PA 17110

Dallas Office
502 N. Carroll Ave. Suite 120
Southlake, TX 76092

New Jersey Office
35 Beechwood Rd. Suite 2A
Summit, NJ 07901

Our Commitment to Vendor Neutrality

Partnering with a firm that brings an independent, objective perspective to every engagement is a top priority for the clients we serve. As an advocate for mission-critical agencies, MCP's commitment is 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 of the entire emergency response ecosystem, free of bias or favoritism to any specific product or service provider. Our recommendations are always based on the value and the benefit provided to the client.

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

Mission Critical Partners Board of Directors

R. Kevin Murray

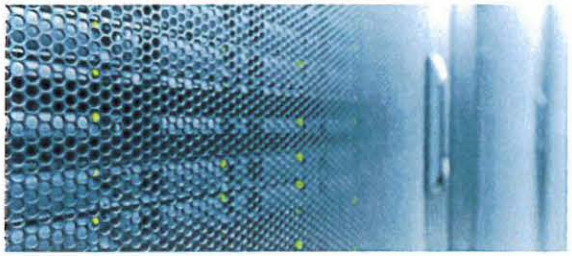
Robert Chefitz

E. Perot Bissell

Bernard Bailey

Douglas Butler

Network and IT Support Services



We help our clients increase the reliability of their network and IT environment long after implementation. Our holistic, IT and network support solutions help our clients realize significant IT cost savings, while remaining confident that their systems are running at peak performance, protected from unplanned network outages.

Clients partner with us so that they can focus on the strategic aspects of managing their public safety operations while we provide expanded continuity, capacity, and capability. We provide solutions that achieve our clients' goals, not their vendors', by applying a technology-independent approach.

With MCP's help maintaining their network environment, our clients have greater confidence that their IT infrastructure and related systems are running smoothly. Our objective is to help our clients drive a greater return from their maintenance investments while reducing their operating expenses. We provide a broad portfolio of assessment, monitoring, and support solutions that improve network reliability and provide agencies with greater insights into their Internet Protocol (IP) network and IT enterprise.

IT Network and Support Solutions	Network Management and Monitoring Solutions	Cybersecurity Solutions	Additional Offerings
Mission-Critical NetInform℠ discovery services	Mission-Critical NetPulse℠ 24x7 network monitoring	Mission-Critical NetInform℠ security assessments	On-request services
Mission-Critical NetInform℠ enterprise IT assessments		Mission-Critical NetPulse℠ security monitoring	IT help desk services
			Integrated vendor support services

These support solutions can provide a holistic, end-to-end view into an agency's entire network and supporting infrastructure with support available for the following networks and applications:

- Computer-aided dispatch (CAD) systems
- Call-handling equipment (CHE)
- Records management systems (RMS)
- Microwave and fiber-optic backhaul systems
- Emergency services IP networks (ESInets)
- Telephony
- 911 and administrative networks
- Environmental site networks

Figure 1: Client-Focused Holistic Support

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.

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 over 17 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.

Cory Bluhm, Technical Project Manager for IT Networks
Technical Program Manager

Cory Bluhm has almost 20 years of experience in the field of Municipal IT, with the last 10 years focused on supporting the critical systems for 911, Fire/EMS, and Police networks. Among his varied experiences, he served as a technical liaison to the Brazos Valley Texas BVCNet which is an organization of local government agencies teamed up to securely link their networks. He continued to expand his technical and managerial knowledge by graduating from the University of North Carolina in 2013 as a Certified Government Chief Information Officer. His broad IT skill set, along with a "can-do" attitude, is beneficial when trying to methodically track down and resolve issues. His time in municipal management honed his personal skills and helps him understand and empathize with government needs such as working within very tight budgets.

Michael Beagles, Senior Technology Specialist
Network Infrastructure Update

Mr. Beagles, Senior Technology Specialist, has been working in the information technology (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 and as the 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).

Dennis Matzen, Senior Manager IT and CAD Technology
Systems Engineer

Dennis Matzen provides subject matter expertise in the technology vision, leadership, and implementation of client IT and CAD programs. He has more than 39 years of diversified experience in the design, installation, and management of computer systems and communications networks for public safety and justice agencies. Dennis' expertise includes in-depth working knowledge and experience of network switching, routing, and security specializing in Windows Server/ Workstation products, virtualization systems, and AIX/UNIX environments. His expertise applies to wireless as well as other more static communications environments. Parallel with his network expertise is his extensive system administration experience spanning Windows and UNIX operating the software, virtualization, and high-availability configurations.

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 Perkins, VP & Director of Lifecycle Management Services Delivery Operations
Client Manager

Mark Perkins has more than 32 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 very large technology company all within the public safety sector. Mark earned his Bachelor of Science Degree from California State University, Long Beach, California, and also carries Quality Management Services (QMS) Certifications in ITIL, TL9000 and ISO9000.

David S. Jones, President, Lifecycle Management Services Division
Customer Advocacy and Quality Assurance

David S. Jones will provide the 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. David directly managed 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. David earned his Bachelor of Science degree in engineering and a Master of Business Administration (MBA) degree in Systems Management.

Resumes

Resumes highlighting the qualifications and experience of the proposed MCP project team are included on the following pages.

Mark Moloney

IT Network Manager, Mission Critical Partners

Mark has extensive experience in providing consultant services to customers in the areas of network security assessment and implementation, network design and support. His background includes working in, wireless networking, data security, data storage design, server, firewall and support of software.

Representative Experience

State Experience

- Florida
  - Support of statewide project network
  - Designing, implementing and upgrading Cisco wireless networks
  - Daily work with Active Directory, Remote Desktop, Windows server 2003, 2008, 2008R2, XP, MS Office 2000-2013, Dell and Cisco hardware, HPOV, Unitrends, McAfee, Cisco Unified Communication and Unity
  - Managing Cisco Prime and Cisco controllers for finding the radius of network accessibility
  - Developed standardized security configurations and backup solutions for Public Safety Two-Way Radio Network
  - Reduced AD, DNS and replication errors on network by 95 percent
  - Work with network monitoring software including, HP OpenView, eHealth, Dell IT Assistant, Openmanage Essentials, FIAL and Zenoss
  - Redesigned active directory and network time to reduce errors and increase manageability
  - Implemented GPOs to standardize and secure the configuration of systems
  - Designed, configured, installed and maintained WSUS for state networks
  - Maintained RSA server and network VPN access
  - Responsible for Cisco Call Manager, Cisco Unified CCX and Unity6 administration and upgrades
  - IT support and training
  - Design, implement and support new office network setup to include, internet link setup, security, data storage, Ad setup and wireless setup and security
  - IT project management
  - Needs assessment, project development and implementation

Industry Experience
17 years

Education
B.S.c. Environmental Engineering

United States Military Academy

Certifications
CCNP
Security +
GSWN
MCSE

Cory W. Bluhm

Technical Project Manager for IT Networks, Mission Critical Partners

Cory is an IT project management professional with extensive experience implementing large software and hardware solutions. He presents solutions that maximize the system's potential. Cory is skilled at delivering highly effective technical product solutions through the use of innovative channels, outlining product benefits in line with client technical requirements. He is able to combine technical knowledge with best practices to deliver second-to-none results in mission critical environments.

Representative Experience

- Operations Manager
  - Performed contract reviews and assisted in navigating the pitfalls of software upgrades
  - Public safety project management
  - Track project deliverables to ensure vendors fulfill contractual obligations
  - Manage and monitor network and software to identify issues prior to outages
  - Monitor systems network and software
- Project Manager
  - Responsible for management of all phases of implementation including engineering development, training, deployment and software support
  - Reviewed contracts, developed and executed project plans
  - Tracked project deliverables to ensure all contractual obligations were met
  - Met with stakeholders
  - Reviewed hardware requirements, predicted growth patterns
  - Troubleshoot issues, explain highly technical issues in nontechnical ways
  - Assisted post project phase support staff resolve issues
  - Trained clients on software, hardware and IT best practices
  - Assisted in client deployments
- Project Experience
  - Orange County Sheriff's Department & City of Orlando, FL– Project Manager for technology integration and migration to new multi-agency 911 dispatch system. Working with IT staff from multiple agencies to identify existing features and requirements, assist with creating the RFP, implement the new solution, evaluate the new system performance and provide ongoing monitoring of the system after cutover.
  - Stockton Fire, CA – Upgrade old dispatch and fire records systems to a new system. Evaluate existing environment, schedule resources, track activity, identify and report project progress.
  - Sacramento Fire, CA –Manager the multi-agency 911 system to identify and document all existing interfaces, work with the new software vendor to ensure capabilities existed and document changes between the systems through implementation phase
  - Warren County, OH – Review new 911 environment and resolve ongoing issues.
  - San Francisco, CA –Manage 911 system upgrade
  - Fort Worth, TX – Monitor existing records system and perform weekly maintenance
  - Midland, TX - Monitor existing 911 system and perform weekly maintenance
  - Alameda Police, CA– Assist with hardware purchase for new 911 system, configure, install and maintain VM environment

Industry Experience

19 years

Education

Bachelor of Arts – International Studies
Texas A&M University
College Station, TX

Bachelor of Arts – International Studies
Austin College Sherman, TX

Certifications

Cisco ICND, Microsoft Professional: Server, AD, Exchange, SQL, Cabling and Network Design Training, Nagios and Solarwinds monitoring, FrontRange Solutions HEAT administrator, Dell technician certified Experience with VMware, NetApp, EMC, HP, UniTrends Backup and Recovery, Extensive Anti-Virus experience, SPIN Sales Training, Crystal Reports Training, FEMA IC courses

Associations

University of North Carolina Certified Government Chief Information Officer

Bryan ISD Technology Board

Michael Beagles

Senior Technology Specialist, Mission Critical Partners

Mike has specialized experience with supporting public safety agencies by providing technical expertise, strategic IT planning, and architecting both on-prem and shared systems for new and innovative mission critical technologies as well as legacy solutions. Throughout his long-standing career, he has worked as a technical service manager providing managed IT services to agencies, a network engineer for several public safety software companies, and as an IT manager with a mid-tier public safety 911/ CAD/RMS/Mobile software provider. His expertise runs deep in services and project management for large and small projects.

Industry Experience
12 years

Education
C-TREC Technical School– CCNA Boot Camp; Security+

Certifications
Cisco Certified Network Associate (CCNA)

MCP/MCTS (Windows Server Administration)

CompTia Security+

Representative Experience

State/Regional Experience

- Minnesota—Project manager supporting DPS-ECN NG911 initiatives and ESInet implementation support.
- Minnesota—Project manager and technical support for DPS-ECN Statewide Text-to-911 rollout
- Pennsylvania Emergency Management Agency (PEMA)—Senior technical consultant and engineer on design and installation of $2M Cisco network in new PEMA facility
- Region 13, Pennsylvania—Technical support for lifecycle managed services
- North Central Texas Council of Government (NCTCOG)—911 network strategic consulting and RFP support

City/County Experience

- Charleston County Consolidated Dispatch Center (CCDC) SC—Lead/participated in collaborative social media pilot with Penn State University and RapidSOS.
- Lubbock Emergency Communications District (LECD) TX—Project manager and technical support for procurement of 911 IPSR; Lead network engineer on 911 network assessment
- City of Cincinnati, OH—Network engineering and incident analysis support
- Cuyahoga County, OH—Project manager supporting county public safety initiatives.
- Hillsborough County, FL—Technical lead, PSAP technology assessment and migration to new public safety operations complex
- Shelby County, TN—911 network assessment and analysis
- Memphis, TN—PSAP network assessment and analysis; project manager for a network overhaul
- Medina, OH—Chief engineer for migration and installation of CAD, RMS, and Mobile Law products hosted in the cloud
- Washington Township, Dublin, OH—IT strategic planning, support services manager

Additional Experience

- EmergiTech IT Manager supporting 911, CAD, RMS, and Mobile applications for departments throughout Ohio, Kentucky, West Virginia, and Tennessee
- The chief technical architect for EmergiTech SaaS platform
- Assistant Terminal Agency Coordinator & LEADS Security Officer for Ohio Law Enforcement Automated Database System.
- Experienced with Criminal Justice Information Services (CJIS) and National Crime Information Center (NCIC) security requirements
- Design and Implementation of end-to-end mobile CAD solution
- Technical support for RFPs on CAD/RMS/911/Mobile system upgrades, and conversions from traditional to Software-as-a-Service (SaaS) models
- Managing and implementing local area network (LAN)/wide area network (WAN) environments with firewalls, routers, and various network equipment

Dennis L. Matzen

Senior Manager IT and CAD Technology, Mission Critical Partners

Dennis has extensive diversified experience in the design, installation and management of computer systems and communications networks for public safety. His expertise includes in-depth working knowledge and experience of network switching, routing and security specializing in Windows server/ workstation products, virtualization systems and AIX/UNIX environments. He brings these experiences and skills to all aspects of every project.

Industry Experience
39 years

Education
AS, Industrial Management

Representative Experience

State Experience

- California
  - Planned, designed, configured and installed advanced networks
  - Established a 24/7 support center
  - Responsible for telephone, radio, data communications and computer network systems
  - Designed, installed and managed the network in support of a large scale, multi-facility campus environment
  - Integrated network with two existing networks in remote location to form a department WAN using TCP/IP Frame Relay Network
  - Technical representative on the transition team to design a new county 911 ECC
  - Served as a senior technical member of the Microwave Master Plan Project
  - Engineering, installation and repair of two-way and microwave radio systems, communications control and related equipment such as antennas, towers, power supplies and multiplex for a countywide communications system
  - Managed daily operations of a branch communications shop.
  - Maintained mobile two-way radios, cellular telephones, two-way base station equipment, trunked radio base stations and controllers, analog and digital microwave radios and associated baseband/multiplex equipment
  - Chief technician to install new communications consoles for three public safety communication centers
- Oregon
  - Designed, installed and supported services for mission critical communications network and computer systems

Chris Faircloth

Business Development Manager, Mission Critical Partners

Chris 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 technology 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. Chris' work involves development, procurement, and implementation of many multi-million-dollar public safety projects. He brings wide-ranging experience in the contractual processes of public safety agencies in several states. Additionally, Chris brings facility and operations experience to the public safety market, with a focus in administration, operations, and technical systems.

Industry Experience
19 years

Education
B.S., Business Administration, University of North Carolina-Greensboro

Associations
National Emergency Number Association (NENA)

Association of Public-Safety Communications Officials (APCO)

Representative Projects

- Coweta County, GA—911 CPE project
- Georgia Emergency Communications Authority—National NG911 grant planning
- City of Atlanta—CAD implementation
- Manatee County, FL—EOC Audio/Video replacement
- Frederick County, VA—Radio System Analysis

Representative Experience

- Regional Sales Director/Territory Sales Manager
  - Supported and achieved implementation of various public safety projects in the southeastern US region.
  - Extensive experience in consulting with customers on the Next Generation Core Services (NGCS) standards and implementation of internet protocol (IP) selective routing.
  - Worked with multiple counties in Florida on the procurement process and implementation of 911 call handling equipment, including multi-PSAP and multi-million-dollar implementations.
  - Led business contractual process and teaming effort with joint-county Project 25 (P25) radio system on the west coast of Florida
- Business Development Manager
  - Consulted and teamed with public safety entities to achieve grant eligibility leading to award for new 800 megahertz (MHz) Motorola system that was interoperable with the state's "VIPER" network.
  - Supported the negotiation and building of a new wide area voice and data system in western North Carolina.
  - Worked extensively on addressing the increasing needs of high-speed mobile data systems and public safety ruggedized mobile data terminals
- Additional Experience
  - Extensive skills in negotiating contracts, navigating political landscape, partnerships and multi-million-dollar initiatives.
  - Develop business plan and opportunities from beginning of implementation, including, support, service, and business development.

Mark Perkins

VP & Director of Lifecycle Management Services Delivery Operations, Mission Critical Partners

Mark is an experienced services professional who oversees the delivery of Mission Critical Partners' Lifecycle Management services to include network monitoring, technical support, service desk and onsite support. His background includes oversight of call center operations, network operation centers, security operation centers, repair services, field service, and managed services. He has significant experience in public safety, telco, and enterprise markets. Mark has had a successful career leading international operations across all continents and is adept at managing both internal and outsourced models to achieve peak organizational performance.

Industry Experience
20 years

Education
B.S., California State University

Certifications
QMS Certification (ITIL, TL9000, ISO9000)

Representative Experience

State/Regional Experience

- Arizona—Assessment of current service and support of communication system, constructed disaster recovery plan for state wide microwave network
- Lubbock Emergency Communications District, TX—Network Assessment, Network Security Assessment
- Region 13 Southwest Pennsylvania Emergency Response Group—Network administration and lifecycle management services of ESInet

City/County Experience

- City of Mountain View, CA—Network Assessment, Network Security Assessment
- Shelby County 911 District, TN—Infrastructure inventory, lifecycle management support
- City of Richmond, VA—Network Assessment
- Wake County, NC—IT Staffing Study
- Lee County, FL—ESInet consulting
- Armstrong County, PA—Lifecycle management support
- Greene County, PA—Assessment of vendor support agreements and incident management
- York County, PA—Infrastructure inventory, network diagrams of systems and lifecycle management support

Additional Experience

- Provided consulting services specific to call center operations, managed services, network operation centers, security operation centers, depot repair, business transformation, and other areas of service delivery including:
  - Project Management
  - Provided capacity and resource planning
  - Designed and implemented "Ground Up" operation
- Director, Network Operations responsible for "Ground Up" design and onboarding of shared network operation center
  - Developed and managed operation budget, policy, and procedures
  - Implemented monitoring system
- Senior Director, Global Device and Board Repair operation
- Director, Call Center Operations
  - Directed operations, cost, and margin performance of call centers, network operation centers, security operation centers.
  - Provided services to public safety and enterprise markets, including federal government agencies, Department of Justice (DOJ)/Department of Homeland Security (DHS)/military branches), state governments, large city and municipal governments, and large retail, livery, and airline enterprise customers

David S. Jones

President of Lifecycle Management Services Division, Mission Critical Partners

President of Mission Critical Partners' Lifecycle Management Services Division, David is a global business executive with experience building high performance organizations. He has achieved consistent results by instilling professionalism and establishing business process improvements and operational efficiency within global and domestic organizations. David's background includes operations and services leadership, strategic and tactical planning, vendor and client relationship management, marketing guidance, contract oversight and directing sales and business development teams. He has worked in the mission-critical communications industry for 35 years for leading firms such as Motorola Solutions, where he established, instituted and launched multiple services and electronic product businesses including biometrics, smartcard, managed services and systems integration businesses with a focus on public safety.

Representative Experience

State/Regional Experience

- State of Maryland—Infrastructure Inventory and documentation and network security analysis
- Arizona—Assessment of service and support structure and processes for their communication network
- Minnesota—Firewall Security Service deployment, support and guidance
- Region 13 Southwest Pennsylvania Emergency Response Group (SWPERG)—Network management, administration, maintenance support and cyber security assessment services of the ESInet
- State of Missouri—Vendor management and maintenance agreement negotiations

City/County Experience

- City of Baltimore—Vendor negotiation and maintenance review
- City of Richmond, VA—Public Safety IT network analysis and recommendations
- Shelby County 911 District, TN—Infrastructure inventory and network documentation
- Armstrong County, PA—ESInet monitoring and lifecycle support services
- Lee County, FL—ESInet Infrastructure monitoring, inventory and network documentation
- Milwaukee County, WI—PSAP relocation and vendor maintenance negotiations

Additional Experience

- Responsible for the successful management and completion of hundreds of radio networks, CAD/RMS, antenna site and other public safety networks and facilities
- Key leader in instituting and launching a systems integration business, critical for the financial turnaround of the public safety business.
- Established, instituted and launched multiple managed service businesses with an initial focus on public safety
- Established services for networks, electronics and site management requirements
- Led a start-up biometrics, software and electronics security company, with an initial focus on international government and public safety solutions
- Aided in the restructure of domestic and global service organizations; restructuring and optimizing global reverse logistics and aftermarket support and repair organizations; analyzing and planning key restructure efforts including outsourcing strategies
- Accountable for the overall P&L, budget and staff of a large services division of a Public Safety equipment manufacturer in North America, overseeing systems integration, field service, program management, field engineering, technical call centers, network operations center (NOC), the security operations center (SOC), reverse logistic repair facilities, sales and business development

Industry Experience

35 years

Education

MBA, Baldwin Wallace College, Ohio

B.S., Civil Engineering, Rose Hulman Institute of Technology, Indiana

Certifications

6-Sigma and Digital 6 Sigma, Motorola Inc.

Executive Management Program, Kellogg School of Business, Northwestern University, Motorola, Inc.

Motorola Management Institute (MMI)

Scope of Work

Phase 1: Mission-Critical NetPulse℠ Advanced (Network & Application Monitoring and Support)

Monitoring

All network links, firewalls, and servers should be monitored for performance and uptime/downtime. The monitoring should provide notifications and trending to assist in proactive network support before issues affect users' experience or cause system outages. This also facilitates planning for growth and troubleshooting issues.

Mission-Critical NetPulse℠ Essential

The proposed **NetPulse Essential** network support service provides Fulton County (County) with a view into its network and enables the County to monitor and support its network's compliance with the Information Technology Infrastructure Library (ITIL) service operation standard. An exclusive and secure environment specific to the County is established within MCP's integrated services platform. All networking devices are discovered and established within the platform's database. This populates the platform's real-time device and circuit health dashboard, enabling the client to have 24 hours a day, seven days a week (24x7) view of device and network performance and alerts. A monitoring profile is deployed to all devices, establishing performance thresholds for alerting. Notification rules are enabled, providing a means for network support personnel to be notified when a device or circuit experiences a failure. Ticketing also is enabled, enabling the County to track all incidents to resolution and track historical patterns of issues and failures. All performance, bandwidth utilization, and fault data are stored in the database, enabling reporting capability with a robust set of data.

Task 1.1: Establish the Network Management Environment

MCP will establish an exclusive and secure network management environment specific to the County. Specifically, MCP will:

1. Establish the environment for the County to facilitate network monitoring, ticketing, and device management.
   a. MCP will configure the environment as required per the definitions defined below.

2. Provide secure access to the County's network management environment for up to four individuals.

3. Provide the County with up to 20 hours of orientation and training for the network management platform, for up to four individuals.

Task 1.2: Configure the Network Management Environment

1. To specifically define the devices to be monitored, MCP will review the proposed monitoring inventory with the County and will make changes at the County's request.

2. To specifically define what processes and elements within a specific device will be monitored, MCP will review the proposed monitoring templates with the County and will make changes at the County's request.

3. To understand the handling procedures for any potential monitoring alarm, MCP will review with the County the proposed support process and will make changes at the County's request.

4. MCP will create a customer support plan specific to the delivery of the network monitoring service to the County. This document will be used as the ongoing delivery document, and will include:
   a. All relevant contact information
   b. Escalation matrices
   c. Notification definitions
   d. Support process flow steps and definition, including planned maintenance process
   e. Monitoring device inventory
   f. Monitoring templates

Task 1.3: Prepare the Network for Monitoring and Test through Burn-In Period

1. MCP will discover items within the management platform as needed for monitoring via Simple Network Management Protocol (SNMP) enabled by the County.

2. As needed, MCP will require Secure Socket Shell (SSH) log in credentials working with the County for this effort.

3. MCP will work with and guide the County regarding how to deploy management agents on all devices as needed for monitoring said devices via a device agent.

4. MCP will test that all devices defined within the network monitoring inventory are connected and are reporting appropriately.

5. MCP will test that all notifications are functioning as agreed to by the County.

6. MCP will test that all actions defined within the monitoring template (e.g., auto-ticketing, notifications) are functioning as defined.

7. MCP will test that all network management platform views extended to the County are working properly.

8. MCP will confirm that report availability is functioning properly.

9. MCP will provide functional reviews on a biweekly basis, via conference calls, with the County through the initial 30-day burn-in period.

Task 1.4: Ongoing Support of Network Monitoring

1. MCP will provide functional reviews monthly, via conference calls, with the County throughout the life of the agreement.

2. MCP will provide support by phone and up to six on-site visits upon request for issues specific to the monitoring service throughout the life of the agreement.

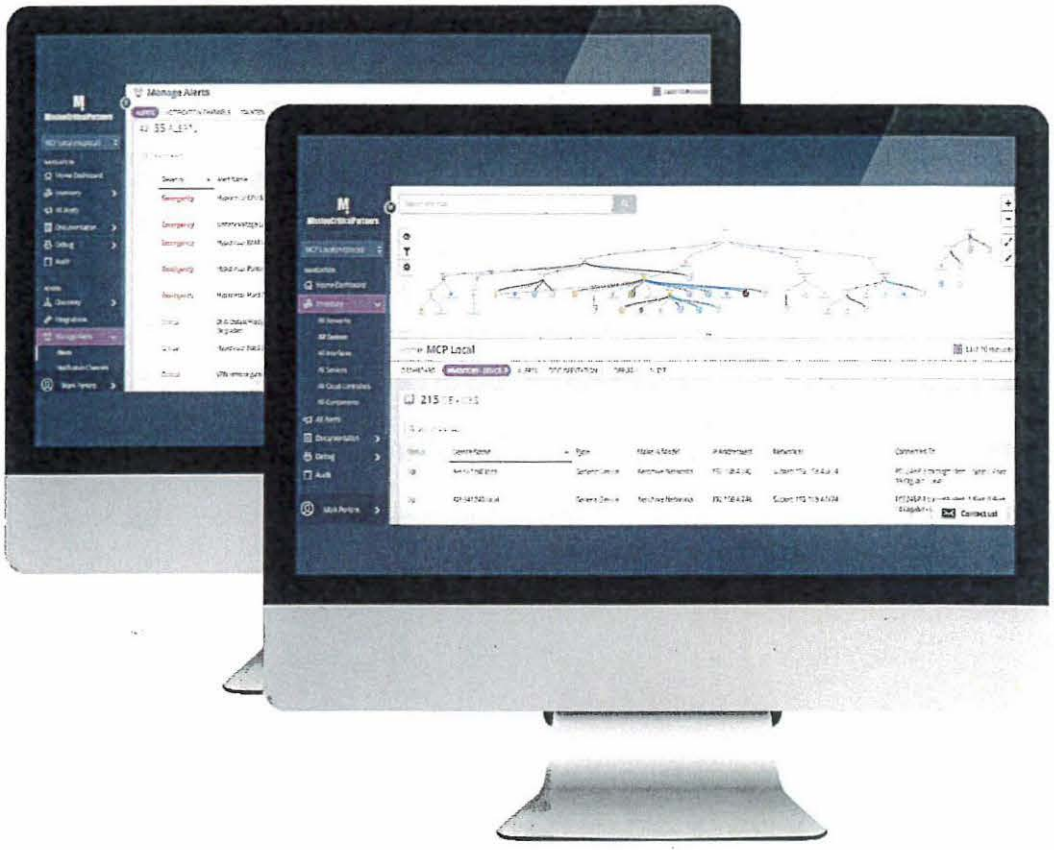


Figure 2: NetPulse Essential

Mission-Critical NetPulse[SM] Advanced Monitoring Services

NetPulse Advanced monitoring services provide proactive and highly responsive around-the-clock remote support services via a network operations center (NOC) that mitigates, escalates, responds and resolves network incidents quickly. Our field engineers and specialists develop a deep understanding of the client's network environment and coordinate with every key network component provider and vendor involved with the network on behalf of the client, acting as a clearinghouse that manages incidents and events until issue resolution.

The NetPulse Advance program includes a comprehensive set of services:

- Establish a secure connection between the agency system and the MCP NOC
- Maintain User Guide – including contact information and help desk instructions
- Provide a help desk to answer your questions, provide advice and solve problems
- Dynamically collect status information
- Set thresholds for alerts
- Monitor the status of systems and network (see below for details)
- Respond when something needs attention
- Analyze and report on conditions – provide monthly reports on routine matters and immediate reports on critical conditions
- Provide recommendations to keep systems and networks functioning properly
- Assist with the operating system and application updates
- Serve as an advocate for the agency when dealing with multiple support providers
- Deploy staff when on-site services are needed

Systems and Network Monitoring

NetPulse Advanced monitoring utilizes a server to collect and transmit data to the MCP NOC services team. The following are representative of the conditions monitored:

Server Monitoring
- Virtual environments
- Processor and memory utilization
- Disk utilization
- Services
- Print queues
- Error reports
- Event logs
- Time sync
- Backup logs
- Logs for high availability disk arrays

Network Monitoring
- Device status (up/down)
- Average response time (ping) to device
- Packet loss to device
- Processor utilization
- Memory utilization
- Port utilization

In summary, MCP monitors the environment and engages as soon as a detected issue requires attention.

Problem Resolution

As issues are identified, MCP follows a triage model, working along with your staff, to isolate the matter into one or more of the following categories:

- Application
- Hardware
  - Server
  - Storage
  - Computer-aided dispatch (CAD) Workstation
- Database
- Virtualization
- Network
- Remote systems and interfaces (not being monitored)

Once the issue is assessed, MCP will either resolve the issue or engage your staff and the other parties involved. MCP will monitor the status until the matter has been resolved.

Communication's and Reporting

Critical issues and conditions are communicated to the agency immediately. Any other monitoring results will be reported monthly at a minimum. The monthly reports include:

- All detected issues
- Corrective actions taken
- Summary of tickets created
- Review of system performance and utilization
- Link to a customized dashboard
- Required site actions

In addition to these communications, MCP assists in organizing monthly status calls that are attended by a wide range of stakeholders including representatives of management, the primary users within the agency, the applications provider, IT support personnel and others.

Help Desk

NetPulse Advanced monitoring includes a comprehensive telephone support desk that is available for reporting issues, requesting services, solving routine matters and answering questions during normal working hours.

The help desk and support are available 24x7x365 for critical matters.

Prerequisites

The success of NetPulse Advanced is based upon the condition and capacity of the environment to support the requirements of the application systems. It is also based upon MCP engineers having an in-depth understanding of the requirements and the environment.

MCP will utilize the results of the recent CAD services assessment to establishing the NetPulse Advance service:

Agency Support and Facilities

The following are needed for MCP to monitor and perform troubleshooting triage of the systems and network:

- Remote access to the site using a virtual private network (VPN) or another secure access facility
- A server to support monitoring – can be a virtual machine
- Ability to send email alerts and reports from the monitoring system to MCP
- Agency contact to assist in coordinating support services
- Onsite assistance during triage and other problem-solving activities

Phase 2: Program Management and Remediation Services

Virtual Machine Ware Environment Replacement

Based on conversations with Fulton County that the current virtual machine ware (VMW) are environment hosting the Public Safety servers cannot be dedicated to them, MCP 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 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 phases.

Task #	Description	Tasks
1	Kickoff meeting	• As part of a remote kick-off meeting, MCP will provide the recommended hardware bill of materials that is compatible with the current environment • Coordinate with the County's IT staff to answer questions and provide technical support.
2	On-Site Installation and Initial Configuration of System	• The MCP program manager will be responsible for the initial configuration of the system hardware.
3	Remote SAN/VMware Configuration	• Created virtual servers as needed • Configure storage as needed • Migrate existing virtual server from the old cluster
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
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 2.1: 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 Fulton resources and MCP
-

Kickoff Meeting Review
Project and task milestones
Schedules and deliverables
Project budget
System technology

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

-
- VMware virtual environment
- Storage environment
- Bill of materials (BOM) for a new system

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

Deliverable(s):

- Project kickoff meeting

Task 2.2: On-Site Installation and 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:

- Install VMware (ESXi) server hardware in client provided equipment rack
- Install storage area network (SAN) hardware in client provided equipment rack
- Cable and label all system connections
  - Power
  - Internet Small Computer Systems Interface (ISCSI)
  - Local Area Network (LAN)
  - Management
  - Keyboard, video, mouse (KVM)
- Initial configuration of SAN
  - Internet Protocol (IP) addressing of all ports
  - Controller parameters
  - Initial Storage Configuration
  - 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

Deliverable(s):

- Server configuration

Assumptions:

- All hardware and software required to support this project will be provided by Fulton County. This will include:
  - VMware ESXi software for new servers, six central processing unit (CPU) licenses required
  - KVM port for ESXi server, three ports
  - Equipment rack for the installation of hardware, 5U (rack units) required
  - Power for hardware, 8 120/240VAC outlets
  - Network switch port for hardware, 22ea 10GBps and 5ea 1Gbps
  - vCenter to manage the new ESXi servers

Task 2.3: Remote 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 form an existing VMware cluster as needed
- Update site documentation to reflect new SAN

Task 2.4: On-Site Cut-Over

The MCP program manager will be responsible for the cut-over 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 have been configured properly to support the CAD applications
- Work with Fulton County and CentralSquare staff to cut over to the new hardware.

Neverfail Deployment

It is our understanding that the county owns Neverfail licenses, and that the product is installed, yet not configured to become operational. Finalizing the configuration and bringing the functionality online will provide necessary backup support to the application that does not currently exist.

Windows Updates

Windows updates should be applied on a regular basis to both workstations and servers after being approved by the IT department and following vendor guidance, and patch levels should be monitored. This protects the system from malware and ensures that all systems are patched to the same level, which eliminates one variable during troubleshooting issues.

Task 2.5: 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 3: On-site CAD Network Support Engineer

In this phase, MCP proposes an on-site CAD Network/Hardware engineer. The resource will be an MCP employee, dedicated full-time to the Fulton County project and in support of the business interests of Fulton County. MCP will be responsible for all employment salary, benefits, taxes and management of this resource.

Responsibilities of this individual include:

- Incident response
- Vendor focal point for county
- Assist in remediation actions
- Root cause analysis
- Coordinate and facilitate monthly status meetings
- Make additional proactive recommendations to improve security and reliability

Project Pricing and Signature Pages

Phase 1: Mission-Critical NetPulse℠ Advanced (Network & Application Monitoring and Support)

Fulton County agrees to purchase NetPulse Advanced monitoring services as described in the scope of work, for a **total fee of $84,000**, including expenses. MCP will invoice the County a one-time establishment of $12,000, and monthly recurring fees of $6,000 at the beginning of each month through year one of the services.

Table 1: Phase 1, NetPulse Advanced Monitoring and Response Fee

Description of Service	Invoice Schedule		Fee Per Year
Year One – Establishment Fee	One-time	$12,000	$12,000
Year One – NetPulse Advanced Monitoring	Monthly	$6,000	$72,000
Year One Total			$84,000

The establishment fee will be paid in-advanced of the NetPulse Advanced monitoring start-up. The establishment fee allows MCP to set-up the networking environment, monitoring profiles and burn-in phase.

Phase 2: Program Management and Remediation Services

Fulton County agrees to purchase the program management and remediation services as described in the scope of work, for the **total fee of $156,400**, including expenses. MCP will invoice the County on a monthly basis on a percent complete basis of all recommended actions.

Table 2: Remediation Tasks Fee

Description of Service	Fee
Program Management and Remediation Services	$156,400
Total	$156,400

Phase 3: On-Site CAD Network Support Engineer

Fulton County agrees to purchase On-site CAD network support engineer services as described in the scope of work Phase 2 services for the **total fee of $288,000**, including expenses. This pricing will be recurring one-month in-advanced and includes all salary/benefits for the MCP engineer.

Table 3: On-site CAD Network Support Engineer Fee

Description of Service	Invoice Schedule		Fee Per Year
Year One – On-site CAD Network Support Engineer	Monthly	$24,000	$288,000
Year One Total			$288,000

Pricing Summary:

The following table provides a summary view of pricing for all services and hardware:

Table 4: Pricing Summary

Description of Service	Fee Yr. One	Fee Yr. Two	Fee Yr. Three
NetPulse Advanced Monitoring and Response	$84,000	$74,200	$76,400
Phase 2 Remediation Services	$156,400		
Year One – On-site CAD Network Support Engineer	$288,000	$296,000	$305,500
Subtotals	$528,400	$370,200	$381,900
Three Year Total			**1,280,500**

Payment terms are proposed to be net 30 days upon the receipt of an invoice by Fulton County.

AGREED TO AND ACCEPTED:

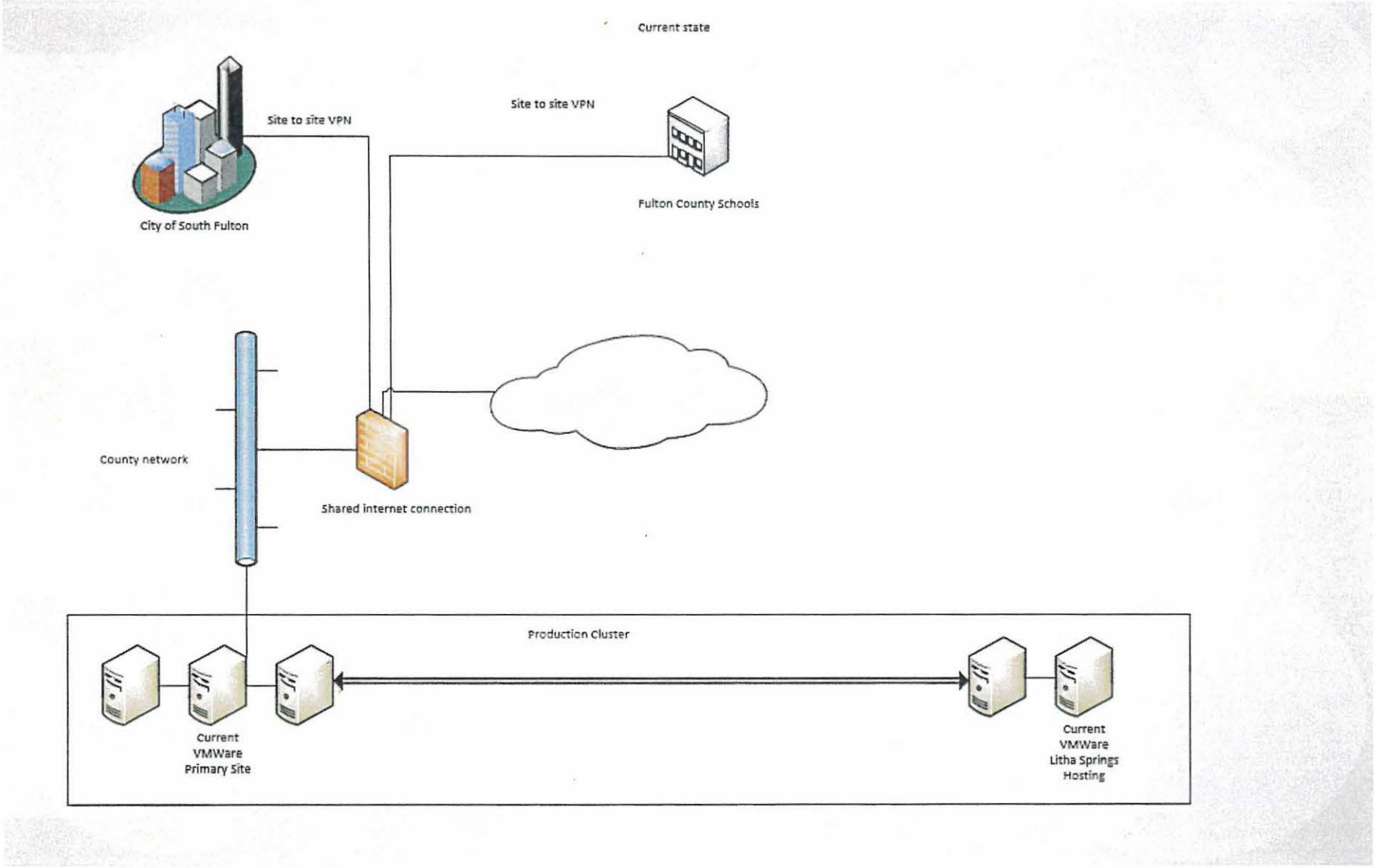
Fulton County, Georgia

Name:
Title: Interim CEO
Date: 1/27/20

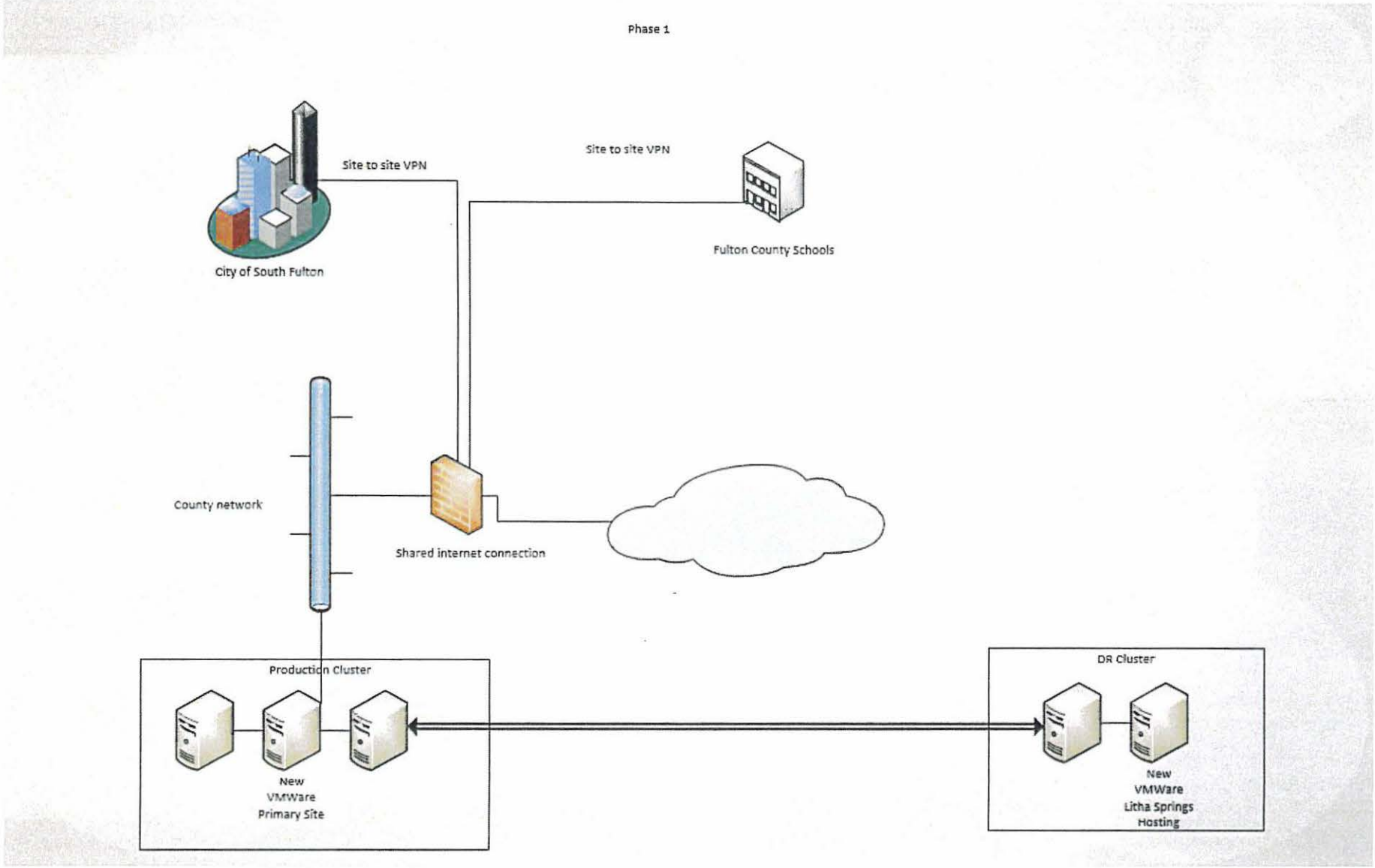
Mission Critical Partners, LLC

Name: R. Kevin Murray
Title: Chairman & Chief Executive Officer
Date: December 2, 2019

Appendix A: Current State Diagram



Appendix B: Phase One Recommendations Diagram



ATTACHMENT C
CERTIFICATE OF INSURANCE

MISSCRI-01 MLORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 12/19/2019

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Rupp & Fiore Insurance Management, Inc. 504 Pittsburgh St Mars, PA 16046	CONTACT NAME:	
	PHONE (A/C, No, Ext): (724) 625-4600	FAX (A/C, No): (724) 625-4680
	E-MAIL ADDRESS: info@ruppfiore.com	
	INSURER(S) AFFORDING COVERAGE	NAIC #
	INSURER A : Travelers Insurance Company	25666
INSURED Mission Critical Partners LLC 690 Gray's Woods Blvd Port Matilda, PA 16870	INSURER B : LLOYD"S OF LONDON	
	INSURER C :	
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY			ZLP51N10683	2/16/2019	2/16/2020	EACH OCCURRENCE	$ 1,000,000
	CLAIMS-MADE X OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	POLICY X PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
A	AUTOMOBILE LIABILITY			BA1N802451	2/16/2019	2/16/2020	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	X ANY AUTO						BODILY INJURY (Per person)	$
	OWNED AUTOS ONLY / SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	X HIRED AUTOS ONLY / X NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
A	X UMBRELLA LIAB X OCCUR			CUP1N917703	2/16/2019	2/16/2020	EACH OCCURRENCE	$ 5,000,000
	EXCESS LIAB CLAIMS-MADE						AGGREGATE	$
	DED X RETENTION $ 10,000							$
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY			UB2N00479A	2/16/2019	2/16/2020	X PER STATUTE / OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y/N: N	N/A					E.L. EACH ACCIDENT	$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000
B	Professional/Cyber			MPL4047321.19	2/16/2019	2/16/2020	General Aggregate	5,000,000
B	Professional/Cyber			MPL4047321.19	2/16/2019	2/16/2020	Occurrence	5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Evidence of Insurance

CERTIFICATE HOLDER

Fulton County, GA
141 Pryor St, SW
Atlanta, GA 30303

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE