WHEN COMMUNICATION IS MISSION CRITICAL

MANAGED SERVICES CAN HELP PUBLIC SAFETY AGENCIES ACHIEVE THE HIGHEST LEVELS OF PERFORMANCE FOR P25 RADIO NETWORKS

When South Carolina faced historic flooding in October 2015, public safety agencies across the state managed 18 breached dams; 500 traffic accidents; 3 major interstate closures; and hundreds of flooded roads, bridges, vehicles and homes. Thousands of vehicles and drivers were stranded, and nearly 150 people had to be rescued. Rural and urban areas faced mandatory evacuations and curfews, and nearly 30,000 people lost power.

South Carolina's efficient emergency response was a bright spot in the midst of this devastation. Powered by an interoperable land mobile radio (LMR) system based on the Project 25 (P25) suite of digital radio communications standards, the state's emergency communications infrastructure was a pivotal tool for managing the record-breaking five-day storm.

To ensure multiple agencies can communicate and collaborate in the event of major disasters, public safety agencies across the country have committed to safer, more effective emergency response by investing in interoperable P25 LMR systems. A managed services approach to the maintenance and support of P25 networks and equipment allows public safety agencies to focus on critical emergency response and community security initiatives while safeguarding against system downtime and cybersecurity attacks.

THE COMPLEXITIES OF MANAGING CRITICAL COMMUNICATIONS NETWORKS

Like any mission-critical technology system, P25 radio networks involve multiple components and network interfaces that must be efficiently managed and supported 24/7 in spite of a dynamic set of challenges, such as:

- **Multiple agency end users.** P25 networks must support the requirements of diverse organizations.
- **Complex management.** IP-based P25 networks are more complex to manage than traditional LMR networks. Skilled network professionals and an industry-leading toolset are needed to monitor and identify critical network events, diagnose and respond to problems, and provide routine maintenance.

- **Rapidly changing technology.** Complex network technology and standards, along with earlier end of support for network components and ongoing software updates, complicate management.
- **Security.** Dedicated security professionals are needed to continuously monitor, detect, analyze and respond to security events and suspicious activities, provide continuous risk assessment and install pre-tested security patches that address vulnerabilities.
- **Limited budgets.** Public safety agencies continue to be challenged by shrinking budgets and higher costs.
- **Skills gap.** Across the public sector, there is a critical shortage of IT and security personnel and skills.

SOLUTION: A MANAGED SERVICES APPROACH

A managed services approach allows public safety agencies to develop an end-to-end service strategy customized to their specific operational requirements. A typical solution might include 24/7 network monitoring, local on-site support, technical support through a service desk, and network hardware repair and restoration with multilevel response procedures.

An operations and support plan that relies on technical, networking and security expertise from a trusted managed services provider enables agencies to maintain network performance targets and service levels, and adapt to evolving technology specifications and standards.

Benefits include:
- Access to a reliable pool of talent and skills
- IT staff freed to focus on agency's mission
- Immediate access to network upgrades, software releases, technology and security patches, fixes, etc.
- Ongoing monitoring of networks and equipment
- Ability to rapidly address disruptions or problems
- Predictable operational expenses

MANAGED SERVICES APPROACH IN ACTION: THE STATE OF SOUTH CAROLINA

South Carolina employs the managed services approach for its 800 MHz trunked network – one of the nation's largest statewide P25 systems. The network provides interoperable communications for more than 700 federal, state, county and municipal governments, emergency response agencies and other entities.

George Crouch, the state's public safety communications administrator, says that this model allows IT staff to focus on the needs of the system's end users instead of working on system maintenance and updates. "We're able to better support users, address issues, and assist in the development of state plans to support interoperability and disaster response," he says.

The state's managed services contract includes a variety of repair and upgrade services, as well as bidding of service contracts related to the operation of the radio system, including generator fuel, air conditioning and heating, electrical, circuit contracts and providing for the physical upkeep of the site compound. "Each of these tasks is time consuming and would otherwise have to be procured or internally managed," Crouch says.

Another major benefit is the fixed pricing structure. "This provides a stable budgeting process and eliminates fluctuations in maintenance costs," he adds.

"The network supported almost 4 million push-to-talk connections during the first 7 days of the flood. It was a record for the system."

— George Crouch, Public Safety Communications Administrator, South Carolina

The performance of the network during the 2015 floods is a testament to the managed services approach. Despite the historic rainfall, only five network sites had intermittent statewide connectivity issues — and these outages occurred when telephone switch boxes were submerged underwater. "The rest of the network performed without any problems and supported almost 4 million push-to-talk connections during the first 7 days of the flood," says Crouch. "It was a record for the system."

Power outages in many areas of the state required the state's managed services partner to constantly monitor and inspect on-site generators, deliver generator fuel and provide on-site technical support throughout the event. Secondly, the managed services team helped public safety agencies who experienced dropped calls and busy signals to identify the radio site creating this issue and transfer these agencies' talk groups to other sites which alleviated the issue.

When South Carolina faced historic flooding in October 2015, public safety agencies across the state managed 18 breached dams; 500 traffic accidents; 3 major interstate closures; and hundreds of flooded roads, bridges, vehicles and homes.

CONCLUSION

Secure, reliable P25 networks that meet performance and business continuity standards are required to support the needs of modern emergency response, but the technical complexities of managing IP networks can challenge public safety agency budgets and staff.

A managed services approach helps public safety agencies keep pace with the demanding requirements of operating P25 LMR networks. Without overtaxing IT staff and budgets, this approach ensures critical network uptime, performance and security while allowing public safety agencies to focus on their most important mission: emergency response and community safety.

This piece was developed and written by the Center for Digital Government custom media division, with information and input from Motorola Solutions.

Produced by:

CENTER FOR
DIGITAL
G O V E R N M E N T

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by:

MOTOROLA SOLUTIONS

Motorola Solutions creates innovative, mission-critical communication solutions and services that help public safety and commercial customers build safer cities and thriving communities. For more information, visit www.motorolasolutions.com/services.

MANAGED SERVICES OPTIONS: A CHECKLIST

☐ Performance targets defined with service level agreements (SLAs) using measurable key performance indicators (KPIs)

☐ 24/7 remote network event monitoring and incident management

☐ Network hardware equipment maintenance, support and repair

☐ Data-driven dashboards that quickly illustrate network performance and services delivered

☐ Network asset management, including cataloguing all network components and developing a proactive life cycle strategy for upgrades, maintenance, repairs and replacement

☐ Security risk assessment to determine the vulnerability of the system, recommend improvements, and develop security and cyber attack response plans and policies

☐ Proactive remote security testing and updates that address newly discovered system vulnerabilities

☐ Continuous security monitoring to identify cyber intrusions and respond accordingly

☐ Special event management and disaster recovery planning, including network support during planned and unplanned events

☐ Dedicated customer, technical and incident support

☐ Onsite and/or remote tech support for troubleshooting infrastructure and equipment problems

☐ Annual preventive network maintenance and testing

☐ End-user equipment/hardware maintenance, support and repair

☐ Network performance optimization, including capacity and coverage optimization and radio frequency/spectrum management