MissionCriticalPartners®

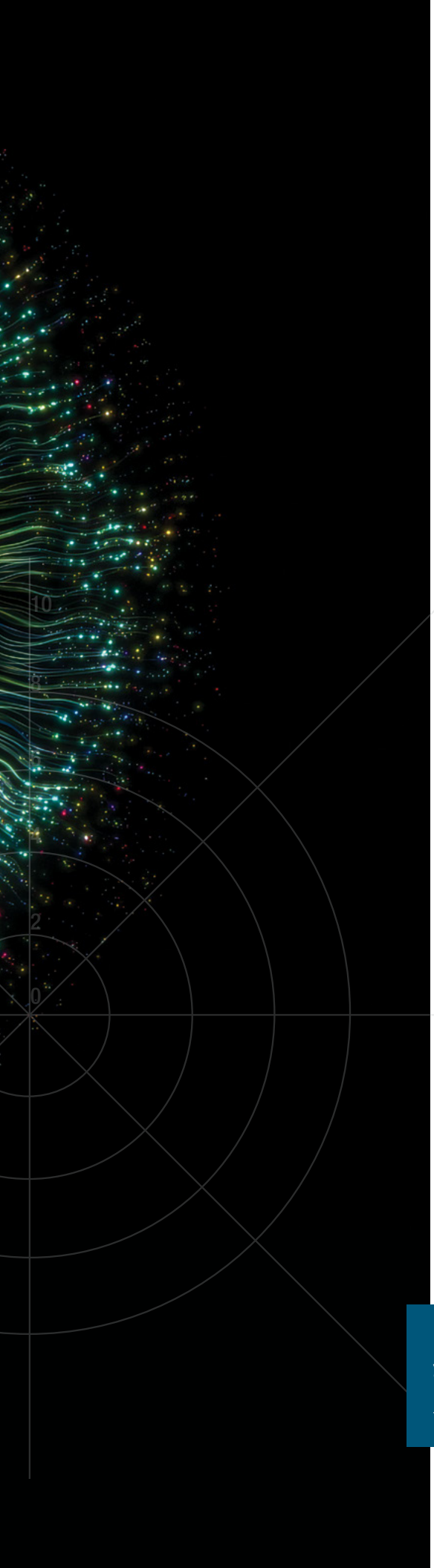
2025 STATE OF THE INDUSTRY

MAPS® The Model for Advancing Public Safety

MissionCriticalPartners®

Mission Critical Partners is a leading provider of consulting and managed services with a vision of helping our clients transform networks and operations into integrated ecosystems that improve outcomes in the public safety, justice, government, healthcare, transportation, and utility sectors. We are committed to helping our clients solve their most pressing challenges.

This third report highlights findings from hundreds of assessments we've completed of the public-sector environment since August 2022. We examine how organizations scored as a whole, explore some of the common challenges they collectively face and where progress has been made, and summarize key trends to watch.



EXECUTIVE SUMMARY

The Model for Advancing Public Safety®, also known as MAPS®, is a proprietary assessment methodology developed by Mission Critical Partners (MCP) for determining where an organization stands concerning numerous critical factors. MAPS® is based on:

- Industry standards
- Best practices
- MCP's collective expertise

MCP aggregated the results of the engagements that were conducted to generate an overarching set of scores for the following critical areas of a public-safety operation:

- Land Mobile Radio (LMR)
- Geographic Information Systems
- Next Generation 911 Readiness
- Operations
- Security
- Staffing
- Data Integration
- Artificial Intelligence
- Organizational Change Management

Understand where your organization stands in key areas and where you need to prioritize your efforts.

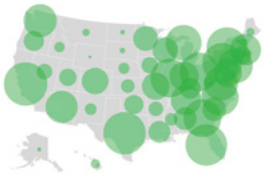
Request a MAPS assessment today.

CHAPTER 01

LAND MOBILE RADIO

Land mobile radio (LMR) systems continue to be the backbone for emergency response communications, both in 911 centers and in the field. On a macro level, they haven't changed much since the ratification of the Project 25 (P25) standards two decades ago, but on a micro level, several changes have emerged that bear watching, including multimodal operation, cloud-based infrastructure, and the negative impact of bidirectional amplifiers.

CHAPTER 02



GEOGRAPHIC INFORMATION SYSTEMS

Geographic information systems (GIS) have played an important role in the public sector for many years, especially in the 911 community, where the data generated by such systems is used to support addressing efforts and to establish emergency-response boundaries. In the Next Generation 911 (NG911) environment, the geospatial data generated by GIS is used to locate callers and dispatch the appropriate response. Despite this importance, use of GIS remains a work in progress.

CHAPTER 03

NEXT GENERATION 911 READINESS

Next Generation 911 systems are still considered a quantum leap forward compared with legacy 911 systems. But while progress has been made in terms of their implementation, they remain very costly, complex, and time-consuming initiatives. One event that promises to quicken the pace is the FCC's order in July 2024 that requires originating service providers to deliver their traffic, at their cost, to delivery points—also known as demarcation points—designated by the 911 authority.

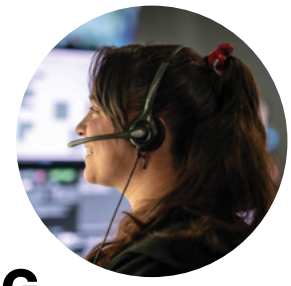
2025 STATE OF

MAPS® The Model for Advancing Public Safety | THIRD EDITION

CHAPTER 07

DATA INTEGRATION

Public-safety systems generate tremendous amounts of data, which only will increase as these systems evolve and new technologies emerge. However, for data to be useful, it needs to be analyzed and contextualized. Once that is done, it needs to be shared seamlessly and in real time with every entity that needs to leverage it—if it doesn't happen, situational awareness and emergency response suffer. Data integration is how it gets done.



CHAPTER
04

OPERATIONS

911 center operations continue to evolve, driven by technological advancements, a persistent staffing shortage, a lack of viable career pathways for telecommunicators, a highly stressful work environment, the need to more efficiently and effectively train personnel, and a desire to operate independently.

CHAPTER
05

SECURITY

The physical security of public-safety facilities, especially 911 centers, generally is solid and has been for quite some time. Cybersecurity is another matter entirely. The bad news is that cyberattackers increasingly are targeting public-sector organizations. Worse, their strategies and tactics evolve at warp speed, in some cases fueled by artificial intelligence. The good news is that public-safety officials have increased their focus on cybersecurity over the past couple of years.

CHAPTER
06

STAFFING

Staffing continues to be one of the most vexing challenges within the public-safety sector, especially the 911 community. However, the situation seems to be improving somewhat, fueled by creative approaches to recruitment, retention, hiring, compensation, and shift configurations. Centers increasingly are reporting that they are close to meeting authorized staffing levels. However, that often is quite different than having the staff needed to perform in alignment with industry standards given their operating environment.

THE INDUSTRY

CHAPTER PREVIEWS

CHAPTER
08

ARTIFICIAL INTELLIGENCE

Excitement regarding artificial intelligence (AI) in the public sector is exploding. However, understanding of the technology and how it can be leveraged to improve emergency-response outcomes remains at a nascent stage. Consequently, public safety agencies should heed the adage that says, “Just because you can doesn’t mean you should” and perform plenty of due diligence before taking the leap.

NEW

CHAPTER
09

ORGANIZATIONAL CHANGE MANAGEMENT

Change is necessary for public-sector organizations to thrive because conditions and environments continually evolve. Organizations that are not innovating and improving their processes are stagnating—and if they’re stagnating, they are not performing optimally. In the case of public-sector organizations, stagnation means that they’re not serving their constituents as well as they could. Unfortunately, organizations and their people steadfastly try to avoid change for a variety of reasons.

METHODOLOGY

MAPS is a proprietary assessment methodology developed by MCP for determining where an organization stands regarding numerous critical factors.

MAPS® is based on:

- Industry standards developed by organizations and workgroups such as the Federal Communications Commission's (FCC) Task Force on Optimal Public Safety Answering Point (PSAP) Architecture (TFOPA), the National Institute of Standards and Technology (NIST), the National Emergency Number Association (NENA), and the Association of Public-Safety Communications Officials (APCO)
- Best practices
- MCP's collective expertise

The 2025 report includes data from assessments completed by MCP since August 2022.

How the MAPS Methodology Works

Since its inception, MCP has conducted hundreds of assessments of clients' technologies, operations, staffing, funding, and governance. These assessments largely have been qualitative based on the experience and knowledge of the firm's subject-matter experts.

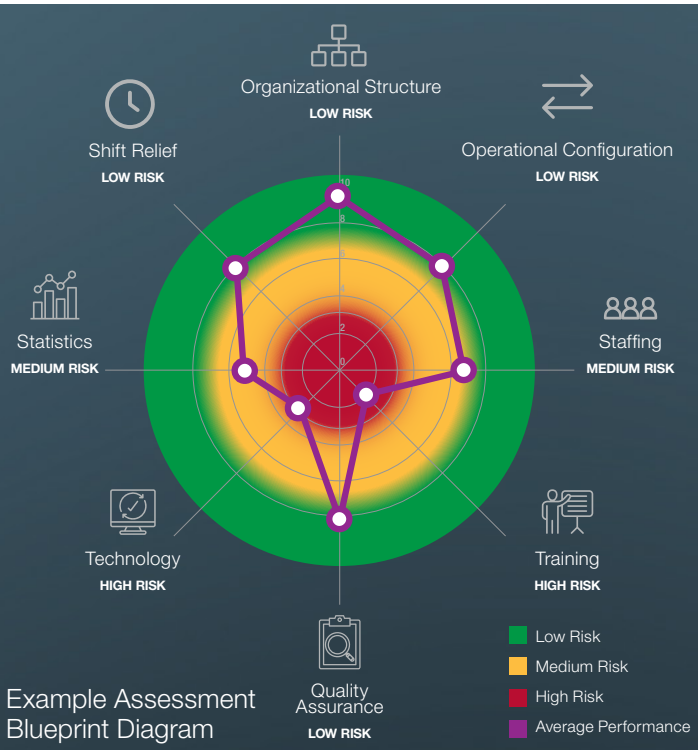
Five years ago, driven by a desire to introduce quantitative analysis into these assessments, MCP launched the MAPS methodology. The methodology — which is based on industry standards and best practices in addition to the firm's collective expertise — enables officials to immediately discern and understand where their organization stands regarding numerous factors.

Question Set

MAPS leverages a quantitative and qualitative question set, and the questions are weighted based on importance. For example, weighting for a technological assessment would consider how likely each factor would cause a system failure. For example, power, transport, and cybersecurity factors would be given greater weight than other factors.

Collaborative Interview

MCP uses the question set in collaborative interviews with an organization's officials and stakeholders. Many questions are asked multiple times to uncover potential discrepancies in the provided answers. Follow-up interviews address disparities and dive deeper into questions for which officials and stakeholders could not provide answers.



Example Assessment Blueprint Diagram

Scoring and Blueprints

A vital element of the MAPS offering is a color-coded blueprint that illustrates the status of each factor that was assessed. The colors are easy to grasp:

- **Green** indicates factors that are at low risk and thus not in need of immediate attention (scores ranging from 7.1–10).
- **Yellow** indicates those at medium risk (scores ranging from 4.0–7.0).
- **Red** indicates factors that are at high risk (scores ranging from 0–3.9).

The MAPS scoring and blueprint become the basis of a comprehensive recommendations report that guides the organization regarding specific strategies for addressing the identified risk factors. The blueprint enables officials to determine where efforts and resources need to be placed to shore up areas of weakness.

The 2025 report includes data from assessments completed by MCP since August 2022.

SCAN TO ACCESS THE REPORT

- MAPS® scoring for multiple industries in public-safety operations
- The 2025 report includes data from assessments completed by MCP since August 2022.
- Sign up for digital access
  (report best viewed on desktop or laptop computer)

ACRONYM LIST

ADA	Americans with Disabilities Act
ALI	Automatic Location Identification
AI	Artificial Intelligence
APCO	Association of Public Safety Communications Officials
CAD	Computer-Aided Dispatch
CHE	Call-Handling Equipment
CJIS	Criminal Justice Information System
COOP	Continuity of Operations
DoS	Denial of Service
DPPA	Drivers Policy Protection Act
DDoS	Distributed Denial of Service
ESInet	Emergency Services Internet Protocol (IP) Network
ECC	Emergency Communications Center, also known as Public Safety Answering Point, or PSAP
ECRF	Emergency Call Routing Function
E911	Enhanced 911
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
GIS	Geographic Information Systems
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
HVAC	Heating/Ventilating/Air-Conditioning
IDS/IPS	Intrusion Detection/Prevention System
IGA	Intergovernmental Agreements
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LVF	Location Validation Function
LMR	Land Mobile Radio
OTAR	Over the Air Rekeying
OTAP	Over the Air Programming
ML	Machine Learning
MOU	Memoranda of Understanding
MSAG	Master Street Address Guide
NFPA	National Fire Protection Association
NG911	Next Generation 911
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NENA	National Emergency Number Association
NGCS	Next-Generation Core Services
OCM	Organizational Change Management
PIN	Personal Identification Number
QA/QI	Quality Assurance/Quality Improvement
REST	Representational State Transfer
SLAs	Service Level Agreements
SOPS	Standardized Operating Procedures
TDMA	Time Division Multiple Access
TFOPA	Task Force on Optimal Public Safety Point Architecture
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network

Mission Critical Partners®

About Mission Critical Partners

Mission Critical Partners (MCP) is a leading provider of data-integration, consulting, network, and cybersecurity solutions specializing in transforming mission-critical communications and public-sector networks into integrated ecosystems that improve outcomes in the public safety, justice, healthcare, transportation, and utility sectors.

For more information, visit MissionCriticalPartners.com

Mission Critical Partners
690 Gray's Woods Blvd.
Port Matilda, PA 16870
Phone: 888.8.MCP.911 or 888.862.7911
Fax: 814.217.6807

YourMissionMatters