2026 STATE OF THE MARKET

Mission Critical Partners®

MAPS: The Model for Public Safety

ARTIFICIAL INTELLIGENCE EMERGENCY MANAGEMENT OPERATIONS GEOGRAPHIC INFORMATION SYSTEMS NEXT GENERATION 911
WORKFORCE OPTIMIZATION GOVERNANCE, RISK + COMPLIANCE LAND MOBILE RADIO OTHER TECHNOLOGIES

20 STATE OF THE MARKET 26

Mission Critical Partners®

MAPS® The Model for Advancing Public Safety

This fourth edition report produced by Mission Critical Partners summarizes where hundreds of state and local public safety organizations stand regarding nine critical aspects of public-safety operations.

About Mission Critical Partners 3

Methodology 4

Insights

CHAPTER 1
Land Mobile Radio: Ensuring Reliable Public-Safety Communications 6

CHAPTER 2
GIS Mapping for Public Safety 11

CHAPTER 3
Next Generation 911 (NG911) 15

CHAPTER 4
Understanding ECC Operations: Modern Challenges and Innovations 19

CHAPTER 5
Understanding Governance, Risk, and Compliance (GRC) for Public Safety 24

CHAPTER 6
Workforce Optimization for ECCs 29

CHAPTER 7
Modernizing Emergency Management for Public Safety 33

CHAPTER 8
AI for Public Safety Staffing 37

CHAPTER 9
Public Safety Technology: Current Trends and Future Outlook 41

About Mission Critical Partners

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 fourth 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.

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

MAPS® 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 2026 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.

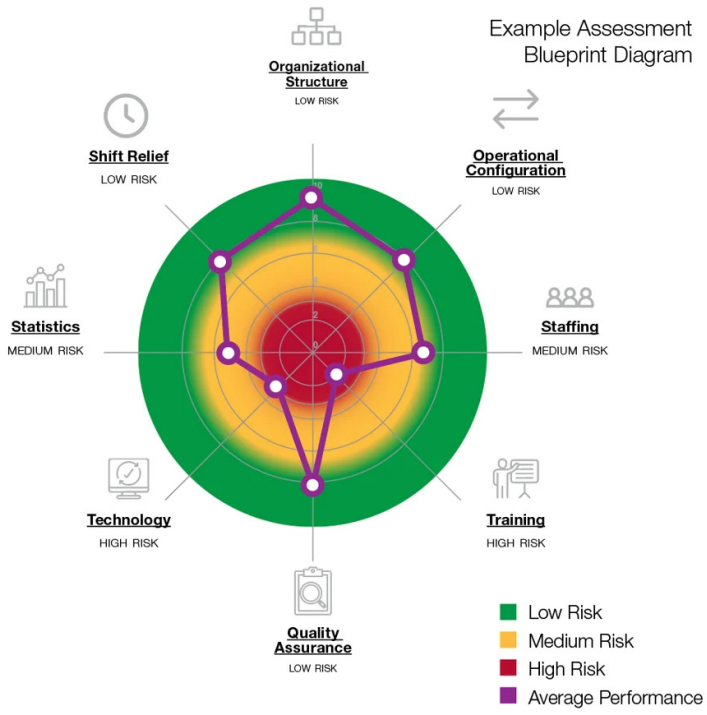
Five years ago, driven by a desire to introduce quantitative analysis into these assessments, MCP launched the MAPS methodology. The methodology — which is based on industry standards and best practices in addition to the firm's collective expertise — enables officials to immediately discern and understand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



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 2026 report includes data from assessments completed by MCP since August 2022.

Chapter 1

Land Mobile Radio

Land Mobile Radio: Ensuring Reliable Public-Safety Communications

Scott Neal
Senior Vice President, Wireless and Court Technology Services
Mission Critical Partners

Nick Falgiatore
PE, Senior Technology Specialist
Mission Critical Partners

The Importance of Modernizing Legacy LMR for Public Safety

Across the United States, legacy land mobile radio (LMR) systems remain essential for public-safety and mission-critical communication, yet many are nearing or past end of life. Equipment obsolescence, deteriorating infrastructure, rising operational demands, and limited lifecycle funding are converging to create significant risks for reliability, resilience, and interoperability. To ensure long-term viability, agencies must pursue coordinated modernization to strengthen LMR communications. This includes system replacement or regional integration, robust lifecycle funding, and structured preventive maintenance.

Challenges Facing Land Mobile Radio Systems Today

LMR systems and voice communications underpin daily operations for first responders, utilities, transportation, and other mission-critical sectors. However, most systems rely on aging infrastructure, unsupported firmware, and subscriber equipment that manufacturers no longer service. Environmental stress on tower sites, outdated shelters, and insufficient backhaul further degrade system performance and reliability.

Coverage challenges remain widespread. While mobile coverage is often adequate, portable and in-building performance is inconsistent due to dense construction, urban growth, and unregulated in-building system installations. The result is operational vulnerability in high-risk indoor environments.

Cost escalation is another defining challenge. Project 25 (P25) systems, while offering modern features, have become prohibitively expensive for many jurisdictions. Total cost of ownership continues rising based on maintenance contracts, proprietary interfaces, software updates, and cybersecurity needs. Subscriber equipment is subject to similar pressures, with standard P25 radios costing $6,000–$7,000 and hybrid LMR/cellular devices exceeding $10,000 before subscription fees.

Cybersecurity risk is increasing as attackers target public-safety infrastructure and LMR systems shift toward IP-based architectures. Many agencies operate with obsolete firmware, inconsistent software updates, limited monitoring, and no dedicated cybersecurity personnel. As devices roam across LMR, commercial cellular, Wi-Fi, and private 5G networks, the attack surface continues to expand.

Despite these challenges, the LMR landscape is entering a transformative period. Multi-network, software-defined communications — blending LMR, cellular, private 5G, and satellite — promise stronger coverage, enhanced resilience, and operational capabilities that bridge the industry to next-generation public-safety communications.

Opportunities for the Future: Transformative Advances in LMR Technology

Hybrid LMR–Cellular Integration for Seamless Coverage – The most impactful development is seamless systems integration between LMR and broadband, enabling radios to automatically switch among networks based on coverage, policy, and operational priorities. This strengthens reliability in buildings, basements, dense urban centers, and remote areas where LMR alone is insufficient. Broadband access also unlocks capabilities such as GPS, mapping, CAD data, images, and video exchange.

Hybrid devices such as Motorola SmartConnect and L3Harris BeOn® are already in the field. Over time, these devices will support intelligent roaming across LMR, commercial cellular, private 5G, Wi-Fi, and satellite networks. Key benefits include:

- Near-continuous coverage without investing heavily in new LMR sites.
- Resilience during disasters or infrastructure failures.
- Greater flexibility in future system design and funding strategies.

Hybrid integration is a foundational step toward next-generation communications.

Private 5G Networks as Cost-Effective Alternatives to P25 – Private 5G networks provide broadband network coverage at significantly lower cost than new P25 sites. A private 5G radio site can be built for 8–10 times less than a P25 trunked site, while supporting data-rich applications beyond LMR's capabilities. These networks integrate easily with hybrid radios and serve use cases such as tribal lands, university campuses, industrial facilities, business districts, and municipal centers.

LEO Satellite Integration for Remote Coverage – Low Earth Orbit (LEO) constellations such as Starlink and Lynk introduce possibilities for direct-to-device satellite connectivity. This technology could extend coverage into remote terrain, wilderness areas, and environments where tower construction is impractical.

Satellite-enabled devices could eventually autonomously prioritize LMR, cellular, Wi-Fi, or satellite signals based on real-time availability.

Challenges remain — including latency, capacity management, device integration, and ensuring continuous satellite availability — but progress is rapid.

Broadband-Enabled Smart Features for Radios – Broadband integration will transform radios from voice-centric devices to multifunction operational platforms. Capabilities include:

- High-speed GPS and mapping.
- CAD incident data pushed to the radio.
- Transmission of images, video, and situational updates.
- Enhanced integration with 911 centers and command staff.

These features improve situational awareness, reduce response times, and strengthen decision-making.

Advanced Features: Automated Drone Deployment – Emerging concepts propose that activating the radio's emergency button could automatically deploy a drone to the user's location. This would provide instant overhead imagery, enhance responder safety, and improve search-and-rescue outcomes. Although early in development, this capability represents a significant operational innovation.

Challenges Facing Land Mobile Radio Systems Modernization

Aging Infrastructure and Unsupported Equipment – Many LMR systems rely on discontinued components, unsupported firmware, and aging analog or early digital equipment. Even P25 trunked systems are reaching the 10-year mark when major upgrades and costly service agreements are required.

Notable issues:

- Inability to obtain replacement parts for older VHF/UHF systems.
- Deteriorating or inadequate shelters, grounding, antenna systems, and microwave backhaul.
- Environmental exposure often leads to catastrophic failures.

Persistent Coverage Gaps in Urban and Indoor Environments – Coverage gaps, especially for portable and in-building use, remain universal. Urban growth, new construction, and unregulated or poorly installed in-building systems degrade signal quality.

Notable issues:

- Conventional systems lack engineered, guaranteed coverage.
- In-building coverage remains inadequate despite National Fire Protection Agency (NFPA) requirements.
- Agencies lack the staff needed to regulate third-party in-building system installations.

Skyrocketing Costs and Vendor Lock-In – The LMR ecosystem has become increasingly expensive and consolidated, with agencies locked into proprietary interfaces and vendor-driven upgrade cycles.

Notable factors:

- P25 system costs are prohibitive for many small and medium agencies.
- Total cost of ownership is rising across maintenance, software, and cybersecurity.
- Vendor dominance (particularly Motorola) drives pricing power.
- Lack of open interfaces limits multi-vendor competition.

Cybersecurity Vulnerabilities in Public-Safety Communications – System reliability is threatened by absent redundancy, insufficient monitoring, and reactive, rather than preventive, maintenance.

Notable issues:

- Growing complexity of the communications network introduces new failure points.
- Maintenance, software, and cybersecurity costs are increasing.
- Few agencies maintain capital reserves or lifecycle funds for system refreshes.
- Vendor-driven obsolescence forces costly upgrades on fixed timelines.
- Workforce shortages limit engineering, technical, and cybersecurity proficiency.

Understanding P25 Interoperability Challenges – Despite P25's standardized air interface, practical interoperability remains limited due to variable compliance, legacy systems, proprietary features, and inconsistent governance.

Notable issues:

- Difficulty coordinating across regions and mutual-aid partners.
- Operational issues with multi-vendor subscriber fleets.
- Reliance on SOPs, governance, and training that often lag technological change.

Addressing Sustainability and Lifecycle Management for Public Safety Systems

Many agencies lack structured lifecycle management for infrastructure, subscriber units, and software agreements. Without proactive funding and planning, systems undergo emergency replacements rather than scheduled modernization.

Notable issues:

- No multi-year refresh plans for radios or infrastructure.
- Software update agreements vary widely and are inconsistently funded.
- Large capital costs arise after long-term service contracts expire.

Subscriber Equipment and Cost Challenges for Public Safety Agencies – Subscriber inventories contain large numbers of obsolete radios lacking encryption, GPS, broadband capability, or current firmware. Replacement costs continue to rise, and some vendors now charge subscription fees tied directly to radio functionality.

Examples:

- P25 radios: $6,000–$7,000
- Hybrid devices: $10,000 or more, plus recurring subscription charges

Criminal Justice Information Services (CJIS) Compliance and Encryption Requirements for LMR Systems – CJIS security requirements mandate that criminal justice information transmitted over LMR systems must be encrypted minimally to the 128-bit standard. Encryption to this standard requires additional costs.

Facilities and Environmental Risks Impacting Public Safety Networks – Tower sites and shelters vary dramatically in condition. Space limitations, inadequate grounding, and failing HVAC systems shorten equipment lifespan and harm system performance. Geographic challenges, especially in rural and mountainous regions, make comprehensive coverage expensive and difficult. Environmental risks include extreme heat/cold, lightning, flooding, hurricanes, wildfires, and tornados.

Cybersecurity Concerns for Public Safety Communications Systems – Risk of cyberattacks is now a major concern as public-safety networks become targets for ransomware and other attacks. Many LMR systems contain outdated software, unsupported firmware, and weak encryption. With limited cybersecurity personnel, agencies depend heavily on vendors.

Risks include:

- AI-driven cyberattacks are becoming more sophisticated.
- Large attack surfaces from end-of-life components.
- Vulnerabilities in IP-based system elements.
- No internal monitoring tools or mitigation capabilities.
- Expanded exposure as radios roam across commercial and private networks.

Emerging Trends in Public Safety Communications Technology

Adoption of Hybrid LMR–Cellular Systems offering seamless roaming and multi-network resilience.

Rise of Private 5G Networks as a cost-effective alternative to P25 expansion and a platform for advanced broadband applications.

Satellite Integration for Coverage Expansion enabling resilient coverage in remote regions and disaster zones.

Broadband-Enabled Smart Radios transforming radios into smart, data-rich platforms that enhance situational awareness and operational safety.

Chapter 2

Geographic Information Systems

GIS Mapping for Public Safety

Robert Horne
Manager - 911 and GIS Technologies
Mission Critical Partners

Claudia Henriquez
Public Safety Specialist - GIS
Mission Critical Partners

Karen Fairchild
GIS Specialist
Mission Critical Partners

What is the Current State of Public-Safety GIS?

Public-safety geographic information system (GIS) capabilities are evolving rapidly, with major opportunities in AI-driven analytics, regional data sharing, indoor mapping and data collection, and modern storytelling through dashboards and story maps. However, agencies face significant challenges: severe staffing shortages, lack of standard operating procedures, widespread data-quality issues, and limited access to critical datasets. These barriers hinder Next Generation 911 (NG911) readiness, reduce analytical capability, and limit the effectiveness of GIS operations in making informed decisions. Preventing GIS data from enhancing emergency response.

An Overview of the Transformation in Public-Safety GIS

Public-safety GIS is undergoing a pivotal transformation as new technologies, operational expectations, and data demands reshape how emergency communications centers (ECCs) and agencies manage spatial information. Significant opportunities exist to improve service delivery, operational awareness, and NG911 readiness.

Artificial intelligence and advanced analytics stand out as especially powerful yet underutilized capabilities. Regionalization and cross-jurisdictional data sharing also represent high-impact opportunities. Greater collaboration, shared datasets, and statewide coordination can unlock multijurisdictional insights and improve resiliency.

Meanwhile, indoor mapping is emerging as a critical need, driven by complex facilities, active-shooter events, and expectations for highly precise location data.

Expanding applications of GIS technology, such as modern storytelling through dashboards and story maps, elevate GIS from a technical function to a strategic communications tool that informs leaders and the public — but demands more from already stretched-thin resources.

Despite these advancements, significant challenges persist, including workforce shortages, inadequate standard operating procedures, poor data quality, and limited access to essential datasets — all of which hinder readiness, efficiency, and innovation.

What Are the Key Opportunities in Public-Safety GIS?

How Can AI and Advanced Analytics Improve Public Safety? – This represents one of the most powerful — and most underutilized — capabilities available to public-safety agencies today. AI can dramatically accelerate pattern detection, improve situational awareness, and reduce the burden on understaffed GIS and ECC operations.

- AI-driven pattern recognition enables early detection of call-volume spikes, geographic clustering of incidents (i.e., hotspots), and trend analysis.
- Automated analytics and reporting can be leveraged to give ECCs actionable intelligence faster and with fewer staff members.

Why Is Regional Data Sharing Important for Emergency Response? – The need for regional coordination of GIS data has been recognized for decades, but most ECCs still operate with a "my area, my data, my problem" mindset. This fragmented approach limits their ability to conduct meaningful analytics, respond effectively to large-scale incidents, and prepare for NG911. Expanding regionalization and cross-jurisdictional data sharing represents a high-impact opportunity with implications for operations, planning, resource allocation, and resiliency.

- Regional GIS operations, enabled by states with strong coordinating bodies, are a key goal.
- Shared analytics across counties and agencies can be leveraged to identify multijurisdictional patterns.
- Cross-agency collaboration is key to removing data silos.

What is the Role of Indoor Mapping in NG911? – This is one of the fastest-growing and most talked-about opportunities in emergency response. Today, major incidents — particularly active-shooter incidents — large campuses, complex facilities, and the increasing expectation of hyper-precise location data have pushed indoor mapping to the forefront. No longer a luxury, indoor mapping rapidly is becoming an operational necessity for ECCs, response teams, and state-level coordinators preparing for NG911.

- Indoor mapping, including layer-based floorplans, room-level navigation, and campus mapping, provides responders with precise navigation inside large structures.
- Integration with NG911-compliant GIS datasets enhances spatial routing.

How Can GIS Be Used for Strategic Communication? – Modern GIS no longer is solely about data creation and analysis. Increasingly, its value comes from how well insights are communicated to leaders, emergency responders, and the public. Without question, people respond better to maps than to spreadsheets — and this is where dashboards and story maps represent a tremendous opportunity to enhance public safety. These GIS software tools elevate GIS from a behind-the-scenes technical function into a front-facing, decision-making powerhouse.

- Dashboards serve as live, interactive operational command environments, integrating spatial and non-spatial data into a consolidated visual interface.
- Story maps help with understanding, persuasion, and policy change, combining maps, photos, timelines, videos, statistics, and narrative text.

Advanced Features: Automated Drone Deployment – Emerging concepts propose that activating the radio's emergency button could automatically deploy a drone to the user's location. This would provide instant overhead imagery, enhance responder safety, and improve search-and-rescue outcomes. Although early in development, this capability represents a significant operational innovation.

What Are the Main Challenges Facing Public-Safety GIS?

How Do Staffing Shortages Impact GIS Operations? – Staffing challenges represent the most significant and pervasive issue affecting GIS operations across the public-safety sector. These limitations impact data quality, NG911 readiness, system integration, analytics, and the ability to adopt emerging technologies.

- Insufficient staffing levels exist across the GIS ecosystem; public-safety agencies often experience difficulties in retaining trained staff, resulting in repeated training cycles.
- High turnover and inadequate job pipelines exist, compounded by few qualified applicants in some regions; compensation disparities; and poor understanding in the workforce about the value of GIS and the career opportunities that exist.

Why Are Standard Operating Procedures (SOPs) Essential? – This is a pervasive and often overlooked challenge in public-safety GIS operations. Where they do exist, they often are outdated, incomplete, or inconsistently applied. SOPs are foundational to operational continuity, quality assurance, and long-term scalability — yet many agencies underestimate their value. This deficiency creates systemic weaknesses at every stage of the GIS lifecycle.

- Many agencies never have documented core GIS processes, believing that they are nice to have but not "must have."
- Lack of SOPs leads to longer training cycles, inadequate knowledge transfer, and an increased risk of data degradation.

What Problems Are Caused by Poor Data Quality? – Geographic data quality is a foundational issue in public-safety GIS. Despite the abundance of available data across agencies, much of it is inconsistent, inaccessible, siloed, incompatible, or unusable for spatial analysis, undermining the effectiveness of GIS operations and slowing progress toward NG911. This is also the most common reason that automated tools fail.

- Common issues include inconsistent naming and forming; missing or duplicated attributes; and incorrect field placement.
- Data exists across numerous systems — computer-aided dispatch, police/fire records management, jail management, public works, permitting, engineering, and more — but rarely flows between them.
- Data often must be transformed before the GIS function can leverage it — but most agencies lack the staff or tools to do so.

What Prevents Access to Critical Public-Safety Data? – A significant barrier to effective GIS operations in public safety is the limited access that GIS staff and analysts have to essential datasets —especially those maintained by 911, law enforcement, fire/rescue, emergency management, emergency medical, and administrative departments. Although these datasets are crucial for building accurate geospatial layers, conducting analytics, and achieving NG911 readiness, they frequently are inaccessible due to cultural resistance, technical restrictions, and organizational misconceptions.

- Many agencies refuse to share datasets with GIS personnel because they believe the information is: confidential; sensitive; legally protected; restricted under CJIS[1] or other compliance frameworks; or too risky to expose.
- Some agencies fear that GIS will reveal slow response times; highlight service disparities between neighborhoods; expose deployment inefficiencies; and identify areas with chronic operational neglect.
- Many leaders do not understand what GIS does. They assume that GIS is about making "pretty maps"; analysts do not need operational datasets; spatial analytics are optional, not essential; and addressing is static, not dynamic.

Trends in Public-Safety GIS to Watch

The Future of AI and Analytics in GIS – AI represents the most powerful and at the same time most underutilized capability available to public-safety agencies. This will change soon in the GIS space.

Regional Data Sharing will Become More Common – This will improve, with key benefits of shared analytics across counties and agencies and elimination of data silos.

Indoor Mapping is Becoming Essential – It's essential due to complex facilities and heightened expectations for precise location data.

GIS Storytelling is Evolving – GIS is evolving from purely technical work to strategic communication, using dashboards for real time, interactive operational awareness, and story maps for public communication, leadership briefings, and policy influence.

1 Criminal Justice Information Services

Chapter 3
NG911

Next Generation 911 (NG911)

Robert Horne
Manager - 911 and GIS Technologies
Mission Critical Partners

Key Challenges and Priorities for Achieving a Fully Realized NG911 System

End-state Next Generation 911 (NG911) hinges on accelerating originating service provider (OSP) migration to Session Initiation Protocol (SIP)-based call delivery, strengthening statewide governance, establishing sustainable long-term funding, and advancing high-quality geographic information system (GIS) programs. Many states still face gaps in technology, cybersecurity, data stewardship, and operational preparedness. While NG911 systems enable the use of multimedia—such as text, videos, images, and precise location data—to provide richer information for emergency responses, they are also becoming more complex and costly. Smaller emergency communications centers (ECCs) or public safety answering points (PSAPs) increasingly must consider consolidation or regionalization to maintain required performance levels.

Why NG911 Governance and Funding are Critical for Success

Throughout the United States, the transition to National Emergency Number Association (NENA) i3-compliant systems requires robust governance structures, stable funding, and accurate GIS data. States with strong, formalized governance frameworks consistently achieve faster NG911 implementation, better vendor oversight, improved funding alignment, and consistent service levels. States lacking unified authorities — i.e., those relying on advisory groups or decentralized leadership — continue to trail in adoption.

Sustainable funding remains a central barrier. Early NG911 deployments often relied on temporary federal stimulus funds without establishing long-term financial mechanisms, creating a looming fiscal cliff as these dollars expire. Modernization of surcharge statutes, expansion of allowable use cases, and removal of legacy restrictions are essential for sustaining NG911.

GIS is the backbone of i3 call-routing but remains underdeveloped in many states. Inaccurate or incomplete GIS datasets undermine routing accuracy — especially in rural jurisdictions that lack technical staff and resources.

Finally, the growing technical and operational complexity of NG911 makes it difficult for small ECCs to operate independently. As a result, many states increasingly view consolidation/regionalization as necessary for resilience, interoperability, and financial viability.

Opportunities to Accelerate NG911 Implementation

FCC Ruling on OSP Migration to SIP-Based Call Delivery – For years, NG911 progress was slowed by originating service provider (OSP) delays in migrating to Session Initiation Protocol (SIP)-based call delivery. The FCC's 2024 demarcation order establishes enforceable requirements and timelines for OSPs once a state 911 authority issues a formal migration request.

- This ruling gives states a mechanism to compel OSP compliance, removing a longstanding barrier to achieving full i3 interoperability.
- Historically, OSPs cited cost, complexity, and competing priorities as reasons for postponement; the new ruling shifts responsibility and accelerates nationwide migration.

Strengthening Statewide Governance for NG911 Success – Governance maturity is the most reliable indicator of NG911 success. Early-adopter states share one common trait: a centralized 911 authority capable of setting policy, aligning funding, ensuring vendor accountability, and coordinating operations. States with decentralized or advisory-only governance consistently lag.

- Robust governance also is foundational for securing sustainable funding. Without a unified state authority, it is exceedingly difficult to modernize funding statutes, advocate for surcharge increases, coordinate lobbying efforts, or educate legislators.
- Governance is the prerequisite for cohesive policy and financial structures that support long-term NG911 functionality.

Modernizing NG911 Funding Models for Long-Term Sustainability – Many states launched initial NG911 components using one-time federal dollars — for example, ARPA[1] funds — without committing to ongoing operational revenues. This created the appearance of NG911 deployment without addressing its long-term sustainment. As temporary funds expire, states face substantial operational and cybersecurity costs that legacy surcharge models cannot support.

- Most surcharges were designed during the analog 911 era, when equipment was cheaper, networks less complex, and cybersecurity requirements minimal. Today's digital environment demands updated fee structures.

1 American Rescue Plan Act.

- States must reassess surcharge levels, expand eligible expenditure categories (e.g., GIS, cybersecurity, cloud services), and remove statutory caps. This is the most direct path toward achieving durable, equitable NG911 systems.

Advancing GIS Programs to Enhance i3 Call Routing – GIS maturity lags other NG911 components across the country, despite its foundational role in i3 routing. Because i3 routing replaces[2] MSAG/ESN entirely with geospatial routing, the accuracy of call delivery depends on the precision of GIS datasets. Inadequate GIS compromises speed, accuracy, and reliability.

- Local jurisdictions — particularly small or rural ones — often lack experienced GIS staff, adequate funding, and knowledge of NG911-specific requirements such as synchronization with NGCS providers, addressing authority standards, and data maintenance cycles.
- Strengthening statewide GIS governance, data-sharing frameworks, and technical support programs offers one of the greatest opportunities to improve NG911 readiness.

Understanding the Key Challenges in NG911 Adoption

How Communication Technology and Information Gaps Impede NG911 Implementation – Despite nationwide progress, many states remain far from full i3 adoption. Approximately one-third of states lack statewide Emergency Services IP Network (ESInet) or fragmented NGCS[3] deployments, continue to rely on legacy selective routers, and operate with limited redundancy and resiliency.

- Some call-handling equipment vendors advertise i3 capabilities but lack full interoperability, contributing to inconsistent performance and increased integration complexity.
- These disparities impede the ability to realize NG911 benefits such as faster, more accurate emergency call routing and improved situational awareness.

Why Cybersecurity Weaknesses Pose a Major Threat to NG911 – Cybersecurity remains one of the most significant threats to NG911 readiness. Even as awareness grows, vulnerabilities persist due to fragmented IT environments, insufficient funding, and overreliance on vendors. The shift to fully IP-based systems means cybersecurity weaknesses can quickly become operational failures.

- Local agencies are especially vulnerable. Most do not conduct regular penetration tests, independent vulnerability assessments, continuous monitoring via a security operations center (SOC), or routine cybersecurity incident exercises.
- In an interconnected NG911 ecosystem, a breach in one ECC can create cascading failures across regions.

The Importance of Training, Policies, and Operational Readiness for NG911 – NG911 is not just a technical upgrade; it represents a fundamental shift in workflow and operations. States with mature NG911 deployments have adapted training, procedures, and operations accordingly. Laggard states show uneven readiness, inconsistent training programs, and limited understanding of new workflows such as multimedia handling, real-time text, and data-driven interoperability.

2 Master Street Address Guide/Emergency Service Number.
3 Next-generation core services.

- Continuity-of-operations (COOP) and disaster-recovery (DR) planning remain weak nationwide.
- Many jurisdictions lack formal plans, rely on outdated documents, or have not adapted to the IP-based NG911 environment.
- NG911's interconnected nature increases the risk of cascading operational disruptions when COOP/DR plans fail.

Addressing the Growing Need for Sustainable NG911 Funding – As NG911 technology becomes more advanced and expensive and 911 revenue declines, many ECCs cannot realistically maintain the required levels of cybersecurity, GIS data accuracy, staffing, redundancy, and technical capability on their own.

- NG911 infrastructure, managed services, cybersecurity, and cloud solutions cost significantly more than legacy systems.
- 911 authorities will need to explore alternative funding mechanisms, such as including it in sales or property taxes.
- Small dispatch centers lack the resources to meet NG911 performance expectations —capabilities that consolidation/regionalization can provide more efficiently, especially in rural areas.

Emerging Trends in NG911 to Watch

Enforcing OSP Migration to Unlock i3 Capabilities – The FCC's ruling gives states the authority to require OSPs to migrate to SIP-based call delivery with device-based location. This is expected to accelerate nationwide NG911 deployment and unlock full i3 capabilities.

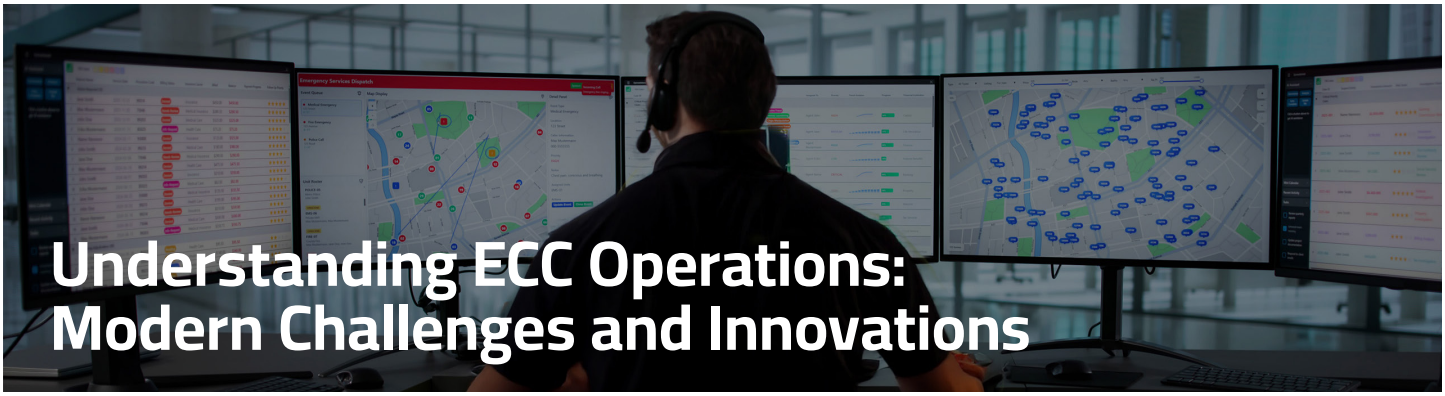
Prioritizing Statewide 911 Governance for Implementation – Statewide 911 authorities remain the strongest predictor of NG911 success. Centralized control enables cohesive governance across policy, funding, cybersecurity, GIS, and operations.

Addressing NG911's Growing Need for Sustainable Funding – With stimulus funding ending, states must adopt modern surcharge models to sustain NG911's higher operational costs. Without action, many "NG911-deployed" states will face significant financial challenges.

Focusing on GIS Maturity to Improve Routing Accuracy – High-quality GIS data is essential for i3 call-routing accuracy. Strengthening statewide programs will be a national priority as states face increasing scrutiny regarding GIS readiness.

Chapter 4

Challenges and Innovations in ECC Operations



Understanding ECC Operations: Modern Challenges and Innovations

Bonnie Maney
Public Safety Communications Operations Domain Manager
Mission Critical Partners

Jason Malloy, MS, ENP, RPL
Operations Domain Leader
Mission Critical Partners

Introduction to ECC Operational Changes

Emergency communications centers (ECCs), also known as public safety answering points (PSAPs), are experiencing rapid operational transformation driven by new technologies, evolving public expectations, and persistent staffing shortages. Leaders are exploring innovative approaches—including alternative-response models and expanded automation—to improve efficiency, reduce emergency response times, reduce workloads, and match resources more effectively to community needs. At the same time, system complexity continues to rise, underscoring the need for modernized continuity planning, resilient infrastructure, and strong organizational leadership. ECCs must therefore balance modernization with sustainability to ensure reliable service in a fast-changing environment.

Why Are ECCs Facing Rapid Transformation?

ECCs across the United States are navigating significant transitions as technology advances, communities demand more diversified responses, and staffing challenges intensify. This environment offers opportunities for improved emergency services delivery but also presents barriers, including resource limitations, cultural hesitation, and integration challenges.

Alternative first response models are among the most transformative developments. These frameworks redirect low-acuity and nonemergency calls to more appropriate resources—311, 211, 988, nurse triage, or civilian response units to name a few — reducing burden on 911 telecommunicators and enabling faster,

specialized assistance. Tools such as AI-based virtual attendants and automated alarm verification further enhance this shift by decreasing manual processing. Leaving ECCs to focus on emergency calls.

ECCs are also beginning to embrace artificial intelligence (AI) and automation, including automated transcription, translation, incident filtering, and workflow support. These tools can significantly lighten cognitive load and improve processing speed, though they require new policies, training, and cultural adaptation.

Despite these advances, staffing shortages remain one of the most pressing issues, affecting training, morale, and operational resilience. Whether from understaffing, short staffing, or both, many ECCs operate with insufficient personnel, limiting their ability to implement new technologies or pursue strategic planning.

Additionally, continuity-of-operations planning (COOP) often lags the realities of modern, cloud-based, interconnected systems. Updated plans are necessary — more than just a simple bug-out plan — to account for today's dependencies across agencies, platforms, and regional networks.

These pressures are reshaping ECC missions, expectations, and capabilities nationwide.

Opportunities for ECCs to Improve Operations

Alternative First Response Models: Benefits and Implementation Tips – Alternative first response models represent a major opportunity to improve ECC efficiency, enhance mission critical service quality, and strengthen telecommunicator wellness. Benefits include:

- Reduced call volume by routing low-acuity and nonemergency calls to 311, 211, 988, and specialized response resources. Reducing nonemergency 911 calls, allowing resources to focus on emergency callers.
- Automation of routine call types (e.g., alarms, abandoned vehicles).
- Integration of diverse response options such as AI-based attendants, nurse triage, mental-health clinicians, and civilian responders.
- Improved workload distribution and reduced burnout by decreasing the number of non-911 call types.
- Improved service delivery to the community by transitioning low-acuity incidents to a more appropriate responder (e.g., public works instead of the fire department, mental-health clinicians instead of law enforcement officers).

ASAP Service: Cutting Alarm Response Times with Automation –

ASAP Service, grounded in the American National Standards Institute (ANSI)-accredited Automated Secure Alarm Protocol (ASAP) and Alarm-Verification Standard (AVS-01), provides automated digital delivery of alarm notifications directly into computer-aided dispatch (CAD) systems and assigns risk-based verification scores. Benefits include:

- Reduced response times — from as high as eight minutes to as low as two minutes.
- Improved data accuracy by eliminating manual transcription errors.

- Enhanced telecommunicator efficiency through automation of high-volume alarm traffic.

How AI and Automation Enhance ECC Efficiency – Emerging automation can reshape ECC operations by increasing call-handling speed and reducing manual tasks. Examples include:

- AI-powered virtual attendants supporting nonemergency lines and select, static location, high call volume-generating 911 incidents (e.g., traffic accidents, structure fires).
- Geofenced incident filtering to automatically manage duplicate calls during large-scale events.
- Automated transcription, translation, and workflow routing.
- Online reporting mechanisms to reduce time spent on the telephone by telecommunicators.

Policy Alignment and Public Education for Better ECC Efficiency – Improved community understanding and interagency coordination are essential to modern ECC operations. Focus areas include:

- Public education regarding appropriate use of 311, 211, 988, and other nonemergency resources.
- Policy alignment between 911 and 988 for consistent collaboration regarding mental health–related incidents.
- Development of community-specific response models tailored to local needs.
- Identification of sustainable funding and governance structures for emerging programs.

Challenges Hindering ECC Progress

Addressing ECC Staffing Shortages: Issues and Solutions – They continue to affect most ECCs, reducing efficiency, morale, and response capability. Notable issues include:

- Many call centers operate below full capacity, causing chronic fatigue, high stress absenteeism, and burnout — even among high-performing teams.
- Training for new hires and continuing education for existing staff members frequently are limited due to insufficient personnel.
- Understaffing and short staffing both affect call-answering times, dispatch performance, situational awareness, and the ability to manage surge events or complex incidents.
- Leadership often prioritizes recruitment over retention, limiting long-term planning and contributing to morale challenges.

Cultural and Planning Gaps in ECC Operations – Strong leadership teams are critical, yet some centers struggle with strategic planning and change management. Notable issues include:

- Lack of long-term technology strategies, which forces ECCs into reactive — and often very expensive — decision-making.

- Telecommunicators feel excluded from decision processes, contributing to resistance and the fear of change.
- Cultural hesitation toward AI-based or automated tools due to concerns about workflow disruption, loss of control, or job security.

Managing Rapid Technology Expansion in ECCs – The accelerating pace of innovation creates substantial operational challenges for ECCs. Notable issues include:

- Vendors often are racing to deploy new solutions and thus are pressuring ECCs to adopt tools without adequate evaluation.
- Personnel, when faced with frequent technology changes, experience frustration and reduced confidence, which leads to change fatigue.
- Limited staff technical expertise exists to test and validate new solutions.
- Increasing system complexity exists as ECC ecosystems expand beyond traditional call-handling, CAD, and radio to include AI tools, online platforms, cloud systems, and advanced interfaces.
- Growing reliance on interfaces exists — such as ASAP service and AI transcription and translation — while helpful, also introduces new risks and the need for new training requirements.
- Mismatch between the speed of technological evolution and ECC comfort levels fuels distrust and slows adoption.

Overcoming Challenges in Alternative First Response Implementation – Alternative first response is a major operational shift but remains conceptually misunderstood. Notable issues include:

- It is not a single product, but a philosophy supported by tools, partnerships, and processes — making implementation inherently complex.
- Early tensions between 911 and 988 created misconceptions about training, competencies, and roles; while improving, some misunderstandings remain.
- Centers sometimes adopt alternative first response capabilities before aligning them with internal procedures, leading to inconsistent implementation or a misunderstanding regarding their proper use.
- Alternative first response requires interoperable systems linking ECCs, CAD, RMS, crisis-care networks, and automation tools, which adds technical and operational complexity.
- Public reliance on 911 persists, even when better-suited resources exist, increasing call strain.

Why ECCs Need Modern COOP Strategies – Modern ECC operations require COOP documents that reflect today's interconnected environment. Notable issues include:

- Outdated COOP frameworks that do not account for cloud systems, Next Generation 911 (NG911) routing, regional sharing, remote operations, or automation for all overflow and abandonment events.
- Increased failure points resulting from expanded technology ecosystems and interdependencies.

- Limited ECC expertise needed to inventory systems, analyze dependencies, or design advanced failover models.
- Need for cross-jurisdictional coordination and specialized technical guidance to create reliable, modern COOP plans.
- COOP plans that still reflect a simple "bug-out" mentality, versus a framework by which an ECC can operate during any type of agency crisis, including the need to evacuate.

Emerging Trends in ECC Operations to Watch

Future of Alternative First Response Models in ECCs – They will continue to reduce 911 workloads, improve wellness, and enable more efficient and specialized service delivery that better meets community needs.

AI and Automation's Growing Role in ECCs – Statewide 911 authorities remain the strongest predictor of NG911 success. Centralized control enables cohesive governance across policy, funding, cybersecurity, GIS, and operations.

Rising Complexity in ECC Technology and Integration – The pace of innovation will continue to outpace the capacity of many ECCs for evaluation and implementation, heightening the need for strategic planning and strong vendor management.

Modernizing ECC Continuity-of-Operations Planning for the Future – COOP updates will become essential to support interconnected systems, cloud-based architectures, regional collaborations, and automated processes.

Chapter 5

GRC for Public Safety

Understanding Governance, Risk, and Compliance (GRC) for Public Safety

Jason Franks
Senior Cybersecurity & GRC Analyst
Mission Critical Partners

Steve Badgio
Vice President & Director of Co-Managed Information Technology (CMIT)
Mission Critical Partners

Why Is a GRC Program Essential for Public-Safety Agencies?

Public-safety agencies operate in an increasingly complex environment where governance, risk, and compliance (GRC) responsibilities are often fragmented and inconsistently managed. As threats intensify and regulatory expectations shift, agencies must transition from reactive, siloed practices to a unified, organization-wide approach. A well-designed GRC program enhances resilience, strengthens informed decision-making, and builds shared accountability — ultimately improving an agency's ability to safeguard its people, systems, and the communities it serves.

What Is the Current State of GRC in Public Safety?

Modern public-safety organizations face mounting operational pressures, rapidly advancing technologies, and expanding regulatory requirements. Yet many still manage GRC activities in isolated pockets, resulting in inconsistent practices and blind spots that adversaries can exploit. A holistic GRC program replaces these sporadic efforts with a disciplined, coordinated approach that improves preparedness, responsiveness, and long-term strategy.

Improved organizational maturity is a key opportunity. While many agencies maintain strong practices within specific departments, processes often vary significantly across the enterprise. Standardizing policies, aligning risk activities, and implementing repeatable workflows help agencies shift from episodic responses to predictable and sustainable risk management. This consistency supports efficiency, accountability, and resilience.

Success also depends on executive leadership and organizational culture. GRC initiatives cannot succeed without sustained engagement from leadership and broad cultural acceptance of continuous risk management. When leaders champion GRC as a strategic priority, agencies maintain momentum through staff turnover, funding fluctuations, and operational disruptions. Embedding GRC into everyday operations ensures it becomes a habitual practice rather than an occasional compliance obligation.

Finally, agencies gain significant value from anchoring GRC programs to established standards and frameworks. Using structured frameworks reduces ambiguity, eliminates gaps, ensures uniform controls, and helps demonstrate due diligence to regulators and stakeholders. The use of GRC platforms and GRC systems helps agencies centralize and automate many of their compliance processes. Collectively, these improvements strengthen cybersecurity posture and increase organizational resilience.

What Are the Key Opportunities for Improving GRC?

How Can Agencies Adopt a Holistic GRC Approach? – Public-safety agencies traditionally manage GRC in silos — e.g., IT handles cybersecurity, the facilities team oversees physical security, HR manages personnel processes, and leadership engages only intermittently. This fragmented structure creates gaps and periods of heightened vulnerability. In contrast, a unified GRC approach:

- Replaces inconsistent or episodic practices with continuous management.
- Enables proactive planning and rapid threat response.
- Breaks down organizational silos and fosters shared accountability.
- Provides leadership with a comprehensive view of organizational risk.
- Holistic GRC encourages collaboration, clarity, and structured oversight, enabling more effective decisions during both routine operations and crises.

How Can Agencies Increase Organizational Maturity and Consistency? – Many agencies rely on pockets of excellence surrounded by uneven processes. Institutional knowledge often is concentrated in a few employees, leaving programs vulnerable to staff turnover and operational disruptions. Improving maturity helps agencies:

- Move away from reactive, event-driven practices.
- Reduce isolated decision-making.
- Apply uniform standards across departments.
- Institutionalize repeatable, documented processes.
- Prevent organizational drift and policy decay.

Standardization ensures that core practices remain consistent regardless of personnel or external pressures.

Why Is Executive Buy-In Crucial for GRC Success?

Leadership engagement and cultural transformation often determine the success or failure of GRC efforts. Without strong executive support, initiatives stall. Without cultural adoption, even well-designed processes fail to take hold. Effective leadership and culture change enable agencies to:

- Elevate GRC as an organization-wide strategic priority.
- Sustain progress through leadership changes, staffing shifts, and funding challenges.
- Develop a resilient workforce that continuously adapts to evolving threats.
- Embed GRC into daily operations rather than treating it as a compliance checkbox.

GRC thus becomes a shared responsibility that permeates organizational behavior.

How Can GRC Frameworks and Standards Be Used More Effectively? – Public-safety agencies operate within a complex regulatory environment involving federal, state, local, and industry-specific requirements. Many agencies struggle to identify which standards apply and how they intersect. A formal GRC program helps agencies:

- Align with established frameworks such as CJIS[1] Security Policy, NIST[2] SP 800-53, and the NIST Cybersecurity Framework.
- Standardize and rationalize controls across departments.
- Reduce inconsistencies, redundancies, and compliance gaps.
- Demonstrate due diligence to regulators, funding bodies, and the public.

Frameworks provide structure and predictability, which are especially valuable in less-mature environments.

What Are the Common Challenges in Implementing GRC?

How to Overcome "Paralysis by Analysis" in GRC Implementation – The complexity of GRC — cross-department coordination, standards alignment, continuous monitoring, risk assessments, risk registers, and regular policy reviews — can overwhelm agencies. This can lead to significant hesitation, delaying action despite escalating threats. Factors contributing to paralysis include:

- Intimidation caused by perceived complexity.
- Limited personnel and time.
- Uncertainty about where to begin.
- Lack of clear executive direction.

Incremental progress and visible leadership support are essential to overcoming these barriers.

1 Criminal Justice Information Services.
2 National Institute of Science and Technology.

What Are the Dangers of an Inconsistent Approach to Risk Management? – Many agencies manage risk only during major events such as facility construction, system deployments, hardware refreshes, or post-incident reviews. Once the project concludes, risk management and compliance often drops off sharply until the next major event — or disappears completely. This creates a pattern of:

- Intense short-term engagement.
- Long periods of inattention.
- A "check the box" mentality that assumes potential risks have been permanently resolved.

Such inconsistency weakens the agency's ability to maintain a resilient cybersecurity and operational posture.

How to Determine Which GRC Standards and Frameworks Apply – Agencies frequently operate under numerous overlapping requirements with little internal alignment regarding which standards apply. Compliance knowledge often is distributed across departments:

- Legal may understand one set of obligations.
- IT another.
- Operations yet another.

No single group typically owns the full picture. Additionally, standards evolve regularly — for example, expanded CJIS requirements, shifting state cybersecurity statutes, or updated federal guidance. Agencies without dedicated compliance monitoring struggle to keep pace.

Even when agencies know the requirements, prioritizing and sequencing them remains a challenge.

How Is the Evolving Cybersecurity Threat Landscape Affecting Public Safety? – Public-safety agencies face significant cybersecurity risks due to their mission-critical operations. Cyberattackers increasingly target these organizations because disruptions can have severe consequences. Key factors include:

- AI-powered cyberattacks that accelerate phishing, reconnaissance, and exploitation.
- Growing emphasis on the human element as the primary attack vector.
- Expanded attack surfaces as agencies implement new systems and technologies.
- Increased complexity in maintaining defenses across interconnected environments.

Continuous training, monitoring, and modernization are required to stay ahead of adversaries.

What Are the Trends in Public-Safety GRC?

Increased adoption of holistic GRC approaches – Public-safety agencies increasingly will adopt coordinated GRC strategies that eliminate blind spots, support continuous monitoring, and improve situational awareness. This shift will integrate processes, enhance visibility, and enable more-proactive management of risk.

Improved organizational maturity and consistency – More agencies will develop standardized processes and institutionalized workflows. This effort will reduce reactive behavior, promote enterprise-wide alignment, and drive more-consistent decision-making across departments.

Enhanced executive buy-in to drive culture change – Leadership engagement will continue increasing as executives recognize GRC as essential to operational resilience and community trust. As the agency's culture evolves, GRC will become part of daily operations rather than an occasional compliance effort.

Greater use of standards and frameworks – Agencies increasingly will anchor their GRC programs in proven frameworks to standardize controls, identify and eliminate security gaps, and enhance predictability across operations.

Chapter 6

ECC Workforce Optimization

Bonnie Maney
Public Safety Communications Operations Domain Manager
Mission Critical Partners

Kyra Pulliam
Project Manager
Mission Critical Partners

Introduction to Workforce Challenges in ECCs

Emergency Communication Centers (ECCs) or Public Safety Answering Points (PSAPs) throughout the United States face opportunities to strengthen workforce performance through structured training, strategic recruitment, improved facilities, and emerging technologies that streamline workloads. Challenges persist, including inconsistent leadership, outdated environments, inadequate compensation, evolving technological demands, and limited wellness support. Purpose-built call centers, modern tools, and professionalized development can boost morale and retention. However, overcoming systemic issues regarding supervision, compensation, and wellness within public safety agencies is essential for long-term workforce stability and resilience.

Overview of Public Safety Workforce and Their Impact

The workforce challenges facing ECCs are increasingly complex, driven by rising public expectations, staffing shortages, technological change, and evolving operational demands. Opportunities are available to improve workforce performance, but persistent obstacles exist that centers must overcome to build stable, resilient teams.

Key opportunities include strengthening training and career progression by establishing a structured framework that clearly defines standards, competencies, advancement pathways, and leadership development. Formalizing these processes helps build consistency, supports succession planning, and reinforces the perception that the 911 profession represents a long-term, credible career.

Recruitment can be improved through more sophisticated screening, stronger branding, and broader outreach — steps that help PSAPs compete in a strained labor market and reduce turnover. Additionally, investments in work environments and purpose-built facilities can significantly enhance morale, reduce fatigue, and improve overall retention. Meanwhile, emerging technologies — including AI-driven tools, virtual attendants, and cloud-based platforms — present another major opportunity by reducing administrative burden, optimizing workflows, and enabling staff to focus on high-priority mission-critical tasks.

However, several structural challenges continue to hinder progress. Leadership deficiencies — such as inconsistent supervision, inadequate preparation for new managers, and rotational leadership structures — create uneven performance and cultural instability. Many ECCs also continue to operate in outdated or poorly designed facilities that negatively affect wellness, increase stress, and exacerbate turnover.

Compensation and benefits often fail to reflect the intensity and responsibility of 911 work, making recruitment and retention difficult. Although new technologies offer significant benefits, they also increase job complexity, necessitate new training, and introduce uncertainty about long-term staffing needs. Finally, many ECCs lack comprehensive wellness programs that address the emotional, physical, and psychological demands of emergency communications.

Opportunities to Transform 911 Workforce Performance

Strengthen Training and Career Development in ECC – Developing a structured, professional training framework is essential to improving workforce performance and retention in PSAPs.

- This includes establishing clear training standards, creating consistent progression paths for each career stage, and providing supervisors and future leaders with dedicated leadership development and not just technical instruction.
- By formalizing these processes, PSAPs can build stronger teams, support succession planning, and reinforce 911 as a professional, long-term career.

Improve Recruitment Strategies for PSAPs – This includes adopting more sophisticated screening methods that assess communication skills, cultural fit, and technological aptitude — not just legacy metrics like typing speed.

- Strengthening brand visibility, promoting the profession's critical role, and reaching broader talent pools help centers compete in a tight labor market.
- A more strategic, structured recruitment approach leads to better hires, reduced turnover, and a more capable workforce.

Upgrade ECC Facilities for Better Morale and Retention – Purpose-built centers — with better lighting, ergonomics, break spaces, decompression rooms, and modern equipment —significantly improve morale, reduce fatigue, and help retain staff.

- Enhanced facilities also support wellness by providing cleaner, safer, and more comfortable spaces.
- As ECCS invest in updated environments, they see measurable reductions in turnover and increased job satisfaction across their teams.

- More call centers are enhancing their workforce optimization significantly by allowing and enabling telecommunicators to work remotely. This approach improves their work/life balance while also expanding the pool of candidates. Providing the necessary infrastructure for this capability also makes bug-out scenarios less troublesome.

Leverage Emerging Technologies to Optimize 911 Operations – The adoption of emerging technologies—especially AI-driven tools—is transforming ECC operations by reducing administrative call volume, streamlining workflows, and freeing staff to focus on higher-priority tasks.

- Virtual attendants, automated triage, and cloud-based platforms can significantly improve efficiency and alleviate staffing pressure.
- Such technologies also increase job complexity, requiring updated training and ongoing evaluation. But when implemented thoughtfully, they are enhancing performance, supporting staffing needs, and strengthening long-term workforce resilience.

Persistent Workforce Challenges for ECC

Leadership Gaps in ECCs – Many ECCs suffer from inconsistent leadership, frequent turnover, and a lack of formal career-focused training for new supervisors.

- Many centers promote high-performing telecommunicators into supervisory roles without preparing them for people management, resulting in inconsistent expectations and uneven policy enforcement across shifts.
- Rotational leadership — common in centers operated by law enforcement agencies or fire departments — further disrupts leadership stability.
- These deficiencies weaken culture, hinder staff development, and contribute to burnout and turnover.

Outdated and Stressful Work Environments – Many call centers operate in outdated, cramped, and/or poorly designed facilities that negatively affect staff well-being and retention.

- Inadequate lighting, ergonomics, space, and environmental conditions contribute to stress and fatigue.
- Conversely, agencies that invest in purpose-built, modern centers — with ergonomic workstations, decompression rooms, improved lighting, and supportive amenities — see significant improvements in morale, performance, and retention.

Compensation and Work-Life Balance Issues – They continue to lag the demands of 911 work, making recruitment and retention difficult.

- Mandatory and last-minute overtime, inflexible schedules, and high local housing costs further strain work–life balance.
- While some agencies are exploring creative incentives—such as housing subsidies, tax relief, or family-friendly policies—these remain unevenly implemented across the country.
- Without competitive pay and supportive benefits, centers struggle to attract and keep qualified staff, worsening overall workforce instability.

Challenges from Emerging Technologies – Emerging technologies — particularly AI-driven tools, virtual attendants, and automated call-handling platforms — are reshaping ECC operations. When implemented thoughtfully, these technologies enhance efficiency and support a more resilient, adaptable workforce. But they also are increasing job complexity.

- These innovations reduce administrative workload and free staff to focus on urgent, complex calls, helping alleviate staffing pressures.
- However, they also increase job complexity, require new training, and introduce uncertainty into long-term staffing models as their full effects still are evolving.

Lack of Wellness Support for 911 Teams – Many ECCs lack comprehensive wellness programs that address the physical, emotional, and psychological demands of the job.

- Telecommunicators often face cumulative stress without adequate resources such as mental-health professionals, structured wellness initiatives, or education for families about the impacts of the work.
- This gap leaves employees vulnerable to burnout and long-term health issues.
- Strengthening wellness support is essential to improving resilience, retention, and overall workforce well-being.

Trends Reshaping 911 Center Workforce Optimization

Professionalizing Training and Career Growth – A major shift in the 911 community is underway toward formalized, structured training programs and clear career progression models. ECCs increasingly are adopting professional standards, leadership development programs, and competency-based advancement to improve performance, retention, and succession planning.

Modern Recruitment Strategies for 911 Centers – More agencies will develop standardized processes and institutionalized workflows. This effort will reduce reactive behavior, promote enterprise-wide alignment, and drive more-consistent decision-making across departments.

Upgrading Work Environments in 911 Operations – A significant trend involves investment in purpose-built, wellness-oriented dispatch centers featuring improved ergonomics and lighting, decompression spaces, and modern equipment. ECCs adopting such upgrades are seeing measurable gains in morale, performance, and retention.

Adoption of AI and Automation in ECCs – ECCs are rapidly adopting AI-driven tools, virtual attendants, automated triage, and cloud-based platforms. These technologies reduce administrative call volume and streamline workflows, helping offset staffing shortages. At the same time, they introduce new training needs and shift job complexity upward. Learn more about the use of AI in public safety.

Chapter 7

Emergency Management for Public Safety

Jason Malloy, MS, ENP, RPL
Operations Domain Leader
Mission Critical Partners

Introduction to Modernizing Emergency Management Response

Emergency management agencies (EMAs) throughout the United States face opportunities to strengthen partner relationships, expand social-media use, adopt drones for faster assessments, improve training and exercises, and modernize procurement for quicker disaster and emergency response. They also face major challenges, including staffing shortages, inadequate facilities and technology, rising disaster frequency, and shrinking federal grant opportunities, as well as state and local funding. Trends highlight growing emphasis on collaboration, real-time public communication, drone-enabled situational awareness, and routine exercises to validate plans and enhance readiness.

How Emergency Management Agencies Operate

Emergency management agencies (EMAs) across the nation at the state and local level operate in an increasingly complex environment shaped by rising disaster frequency, expanding responsibilities, and widening resource gaps. Consequently, stronger collaboration, modernized tools, and sustainable investments to enhance preparedness and response capabilities are sorely needed.

A major opportunity lies in strengthening relationships with fire/rescue, law enforcement, emergency medical, emergency communications centers, public works, and other stakeholders. Proactive engagement — through regular meetings, joint planning, and coordinated exercises — builds trust, clarifies roles, and improves interoperability before disasters occur. These relationships become

essential during high-pressure incidents, enabling smoother communication and more efficient resource sharing.

The growing importance of social media, as both a communication channel and situational awareness tool, is a key trend. When used strategically, social-media platforms provide EMAs with rapid, low-cost ways to issue alerts, counter misinformation, monitor citizen reports, and identify emerging needs when traditional systems are overwhelmed.

Technology, particularly drones, represents another significant opportunity. Drones enable faster, safer post-disaster assessments; enhance search and rescue through live video feeds and thermal imaging; and deliver critical supplies to isolated areas. For many resource-constrained jurisdictions, drones offer a cost-effective way to expand operational capabilities without placing responders unnecessarily in unsafe or untenable situations.

Meanwhile, significant challenges exist. Staffing shortages, inadequate facilities, aging technology, and shrinking federal grant opportunities — as well as state and local funding — strain agencies' ability to meet growing demands. Further, many EMAs lack the specialized skills, personnel, or financial resources needed to sustain advanced capabilities or keep pace with operational expectations.

What are the Key Opportunities in Emergency Management Agencies?

How Can Agencies Strengthen Stakeholder Integration in Emergency Management? – A major opportunity lies in proactively building and maintaining strong relationships with fire/rescue, law enforcement, emergency medical, public works, and other. These relationships should be solidified with partners before disasters occur to aid in disaster recovery. Specific tasks include:

- Establishing regular engagement with fire/rescue, emergency medical, law enforcement, 911 centers, and public works.
- Conducting joint emergency planning and exercises to improve coordination and communication between local and state governments and federal agencies.
- Sharing capabilities and resources, especially in small or understaffed jurisdictions.
- Strengthening trust and communication channels to enable faster, more effective response during emergencies.
- Establishing and executing hazard mitigation plans.

What are the Opportunities for Using Social Media in Emergency Management? – Leveraging social media offers fast, low-cost public communication (e.g., boil-water notices), crowdsourced situational awareness (e.g., reports of blocked roads or downed power lines), and real-time monitoring of citizen reports during disasters. Doing so also:

- Helps identify urgent needs when 911 is overwhelmed.
- Supports damage assessment, as well as tracking damage patterns and emerging hotspots.

How are Drones Being Leveraged in Emergency Management? – Drones, or an unmanned aerial vehicle (UAV), offer EMAs faster, safer damage assessment, improved situational awareness, and enhanced search and rescue (SAR) through live video aerial feeds, mapping data, and thermal imaging, drastically reducing response times. They also can deliver critical supplies to isolated areas. Though adoption varies, drones provide a cost-effective way to expand capabilities for resource-constrained jurisdictions and are becoming an increasingly valuable emergency-management tool.

- Drones as first responders (DFR) after storms, floods, wildfires, or tornadoes, enable emergency managers to understand the scale and severity of damage far faster than traditional ground-based assessments.
- Responders can use drones to locate individuals trapped under debris, stranded in flood waters, or lost in remote areas—often without placing personnel in hazardous conditions. Drones can deliver critical supplies — such as medical materials, food, or communication devices — to areas cut off by flooding or debris.

Why is Enhanced Training a Priority for Emergency Management Agencies? – Training and exercises vary widely across jurisdictions, with many lacking staff, funding, or time to conduct them consistently. Yet even simple drills improve coordination, clarify roles, and reveal capability gaps. Effective after-action reviews and HSEEP-based1 planning strengthen preparedness, making routine exercises a critical opportunity for enhancing emergency management readiness.

- Exercises, even simple tabletop sessions, are among the most effective tools for improving coordination, validating and improving plans, and identifying capability gaps before real-world incidents expose them.
- Exercises provide opportunities to practice disaster assessment, evacuation procedures, shelter operations, and continuity of operations — tasks that cannot be mastered without hands-on experience.

What are the Key Challenges Facing Emergency Management Agencies?

Widespread Staffing and Workforce Shortages – EMAs across the country face persistent and widespread staffing difficulties, many of which mirror the challenges seen throughout the public-safety sector but are compounded by the unique nature of emergency-management work.

- Many EMAs are underfunded, understaffed, or staffed by personnel performing multiple roles.
- Emergency management requires unique skills, making the candidate pool smaller.
- Even when someone can be retrained into the role, the required competencies — coordination, logistics, planning, disaster operations — are highly specialized and thus limit recruitment.

Facility and Technology Constraints – EMAs nationwide face significant limitations in their physical spaces and supporting technology, many of which hinder their ability to coordinate effectively during disasters. Such constraints reduce efficiency, slow decision-making, and weaken an agency's ability to maintain situational awareness during emergencies.

- Many emergency operations centers (EOCs) are not purpose-built; they often

are crammed into repurposed spaces such as police department basements, fire department training rooms, or conference/training rooms.

- In many jurisdictions, the EOC and emergency communications center (ECC) are in different buildings or separated by floors within the same building, which prevents or severely limits constant, high-intensity communication and coordination during disasters.
- The use of social media during disasters continues to be affected by limitations, including misinformation, unequal access (i.e., the digital divide), and the lack of analytics capabilities.
- The use of drones can create regulatory issues (e.g., compliance with FAA rules), public privacy concerns, and training and data-management burdens, which can be barriers to adoption, especially in small EMAs.

Increasing Disaster Frequency and Operational Demands – EMAs are experiencing growing operational pressure as disasters become more frequent, more severe, and more complex. This trend affects jurisdictions of all sizes, from large metropolitan areas to small rural counties, and it compounds other longstanding resourcing and capability challenges.

- The surge in disaster activity places substantial strain on EMAs that are already understaffed and underfunded.
- As the number of incidents grows, EMAs spend larger portions of their time in some stage of recovery, reducing their ability to conduct planning, exercises, and training.

Persistent Funding and Grant Challenges – EMAs are experiencing significant and growing challenges related to funding, grants, and long-term financial sustainability. These issues affect nearly every aspect of operations, from strategic planning and facilities to staffing and technology.

- Many jurisdictions perceive a decline in available grant dollars and face intensified competition for remaining funds, creating a de facto funding cliff for capabilities initially built using grant funds.
- Many EMAs lack dedicated grant writers; financial analysts; staff trained in federal procurement, grant management, or reporting; time to prepare quality applications.

Emerging Trends with EMAs

Strengthening relationships and stakeholder integration –Joint planning, shared resources, and regular engagement are becoming foundational to improving disaster readiness and collaborative operations.

Better use of social media – The platform continues to grow as a critical tool for real-time communication, crowdsourced reporting, rumor control, and rapid distribution of alerts.

Increased leveraging of drones – They are transforming emergency management and represent a significant technological trend reshaping response operations.

Enhanced training and exercises – More jurisdictions are recognizing the value of consistent, scalable training and exercises—even simple tabletop drills—to strengthen coordination, validate plans, and identify capability gaps.

Chapter 8

Artificial Intelligence

The Role of AI in Addressing Public Safety Staffing Shortages

John Chiaramonte
President, Enterprise AI Strategy
Mission Critical Partners

How AI is Mitigating Staffing Pressures in Emergency Communication Centers

Public-safety agencies, especially emergency communications centers (ECCs), face severe staffing shortages, and artificial intelligence (AI) and machine learning are emerging as a key tool to reduce call volume, speed call processing, and improve telecommunicator performance. Embedded AI capabilities are rapidly entering mission-critical systems to transform public safety by enabling automation, decision support, and multimodal analysis. However, reliability issues, cultural distrust, and the absence of clear governance hinder adoption. Agencies need standards, oversight frameworks, and improved data management to use AI advancements safely and effectively.

The Integration of Embedded AI in Mission-Critical Systems

Public-safety agencies, especially emergency communication centers (ECCs), continue to struggle with persistent staffing shortages that increase workloads, slow call processing, and heighten burnout. AI is emerging as a critical tool to mitigate these pressures. Early deployments focus on intercepting and triaging nonemergency calls, reducing the burden on telecommunicators, while advanced transcription and real-time language translation are improving accuracy and lowering cognitive load. Beyond call handling, AI is increasingly used to enhance telecommunicator performance through automated quality assurance, rapid post-call evaluation, and emerging voice-analysis tools that can signal stress, fatigue, or potential burnout.

A major shift in the past year is the transition from standalone AI products to AI embedded directly within mission-critical systems such as CAD and call-handling platforms. Embedded capabilities — like predictive search, automated summaries, and voice-activated workflows — are accelerating adoption because they require little integration work from agencies. At the same time, AI enabled automation and decision-support functions are transforming operational awareness, enabling pattern detection, resource deployment, and multimodal analysis of audio recordings, video footage, and sensor data.

Despite rapid progress, reliability challenges — such as hallucinations, bias, and inconsistent performance — remain significant barriers. Cultural resistance, public skepticism, and the absence of clear standards or governance frameworks further complicate implementation. Developing oversight, transparency practices, and improved data management will be essential as AI integration accelerates across the public-safety landscape. Allowing agencies to leverage AI to improve public safety through operations.

What Are the Key Opportunities for AI in Public Safety?

AI Can Ease the Impact of Staffing Shortages – Public-safety agencies across the country continue to grapple with severe and persistent staffing shortages. ECCs remain particularly vulnerable, as vacancies among telecommunicators increase call-processing times, drive burnout, and degrade service levels. AI presents some of the most promising opportunities to relieve this pressure — although progress has been slower than many anticipated.

- AI technology is being used in some ECCs to intercept, classify, and triage nonemergency calls before they reach a human telecommunicator. This can significantly reduce call volume and free personnel to focus on higher-priority incidents.
- Transcription and real-time language translation capabilities have advanced substantially in the last year and are being leveraged to lessen the cognitive burden on telecommunicators, reduce call-processing times and improve service delivery, and eliminate errors.

AI Can Improve Telecommunicator Performance and Well-being – An equally important opportunity lies in AI's ability to boost human performance in high-stress, time-critical environments. AI-supported performance tools — particularly in the areas of quality assurance, training, and call analysis — already are making measurable strides, even if adoption remains slower than anticipated.

- AI can be used to evaluate every call shortly after completion, providing immediate feedback to telecommunicators and enabling training that is better aligned with real deficiencies.
- Though still at a nascent stage, AI can be used to perform telecommunicator voice analysis (tone, cadence, inflection) to flag potential burnout, cognitive overload, and indicators of an impending meltdown.

AI is Being Embedded into Existing Systems – A year ago, agencies tended to view AI as a standalone technology —something they would "buy" as a dedicated tool, like transcription software or a separate analytics engine. Today, however, AI is no longer purchased as a product. It has become an embedded capability

woven into the systems and software ECCs already rely on every day. This shift is transformational.

- Examples include AI-powered search and query features inside CAD systems; embedded transcription within call-handling platforms; voice-activated commands for navigating databases; summaries automatically generated from call or incident data; and predictive prompts that help dispatchers or call-takers surface relevant information faster.
- Historically, ECCs avoided deploying standalone AI tools because they required budget authorization and workflow redesign, i.e., telecommunicators don't want to deal with yet another attention-sapping screen or application. In contrast, embedded AI arrives pre-integrated, with most of the technical work done by the system vendor.

AI-Powered Automation and Decision Support – AI is rapidly reshaping how public-safety agencies, and justice organizations process information and make decisions, to enhance speed, accuracy, safety, and situational awareness. At the same time, agencies are discovering that advanced automation and machine learning does not replace human judgment — rather, it amplifies it, enabling personnel to make faster, more informed decisions in high-stakes environments.

- AI's ability to detect patterns across billions of data points enables automated identification of emerging threats or complex situations more quickly than humans can.
- AI's multimodal capabilities — integrating text, audio, images, and video — enable robust decision support for ECC personnel and field responders, e.g., interpreting live surveillance footage or drone feeds to identify hazards or analyzing "alert-rich" environments (alarms, sensors, body-worn cameras) for decision-making cues.

What Are the Main Challenges of Implementing AI in Public Safety?

AI Reliability a Major Obstacle — Reliability is one of the most significant obstacles preventing public-safety agencies from fully embracing AI. These issues fall into several interconnected categories: accuracy, hallucinations, bias, reasoning limitations, prediction-driven behavior, and inconsistent performance across tasks. Each of these reliability shortcomings introduces risks that are unacceptable in environments where consequences can include delayed response, misdirected resources, legal exposure, or public mistrust.

- Up to 25 percent of AI responses may be incorrect, misleading, or entirely fabricated, depending on the use case. This is highly problematic because a single incorrect output could influence dispatching decisions, prioritization, or interpretations of critical information. Data bias, though improving, is a significant factor.
- AI models predict, but don't "think." They can replicate patterns but cannot replicate human reasoning; they struggle with multi-step logical deductions, and they may fail basic relationship or context inferences that a human would consider trivial.

Cultural and Trust Barriers Hinder AI Adoption – While technical issues such as hallucinations and data quality pose quantifiable risks, human concerns — ranging from fear of job loss to skepticism about fairness — are far more difficult to overcome. They slow adoption, limit pilot success, and shape agency attitudes toward AI integration.

- Many public-safety professionals — especially veteran staff members — do not understand how AI works, what its limitations are, or how it produces results.
- Public-safety professionals are trained to avoid mistakes because errors can cost lives or lead to legal consequences. This makes them inherently skeptical of AI.
- Another factor that fuels skepticism concerns the current AI financial model, which is unsustainable — what happens when a 911 center depends on an AI tool and its vendor goes bankrupt?

Lack of Governance a Risk for AI in Public Safety – While AI adoption is accelerating across the public-safety sector, the development of standards, policies, and operational guardrails has not kept pace. Agencies are experimenting with AI tools — sometimes intentionally, sometimes because AI has been silently embedded into the software they already use — but most do so without fully developed guidelines or governance structures. This gap increases organizational risk, slows adoption, and undermines trust.

- Unlike long-standing areas such as computer-aided dispatch (CAD) and call-handling, there are no consensus standards for using AI in the public-safety environment.
- AI requires human oversight and likely always will, but no framework exists for this purpose. Lacking defined oversight best practices increases liability risk and erodes staff confidence. Similarly, transparency requirements are not defined across the sector, e.g., agencies lack standards for explaining how AI reached conclusions.

Key AI Trends to Watch in Public Safety

AI is Addressing Staffing Shortages in Public Safety – Public-safety agencies, especially ECCs, are facing severe staffing shortages, and AI is increasingly being used to offset these gaps.

AI Tools Enhance Telecommunicator Performance and Well-Being – AI is expanding beyond call filtering to tools that directly support human operators.

AI Features Embedded in Mission-Critical Systems – Instead of buying standalone AI products, emergency services agencies now receive AI features embedded within systems they already use.

AI Advances Automation and Decision-Making – AI is rapidly reshaping operational decision-making. Increasingly, it is being perceived not as a replacement for human judgment but as a tool that amplifies speed, accuracy, and context in mission-critical environments.

Chapter 9

Technology in Public Safety

Public Safety Technology: Current Trends and Future Outlook

Robert Horne
Senior Technology Specialist
Mission Critical Partners

John Chiarmonte
President, Enterprise AI Strategy
Mission Critical Partners

Jack Dougherty
Manager, Public Safety Applications
Mission Critical Partners

Bob Scott
Automated Systems Domain Leader
Mission Critical Partners

An Overview of Emerging Public Safety Technologies

Public-safety technology is rapidly evolving across computer-aided dispatch (CAD)/records management systems (RMS), call-handling systems, and unmanned aerial vehicles. CAD/RMS platforms increasingly emphasize integration, cloud migration, and mobility, enabling seamless data sharing and field access via native mobile applications. Cloud-based call-handling equipment (CHE) solutions offer scalability and resilience but still are immature, suffer from latency issues, and require robust, redundant connectivity. Drone use is expanding significantly, especially through Drones as First Responder (DFR) programs, which provide situational awareness and reduce unnecessary responses. Recent Federal Aviation Administration (FAA) reforms have streamlined the drone waiver process, dramatically accelerating nationwide adoption. However, it is prudent that agencies develop sound policies before they are deployed.

What Are the Latest Innovations in Computer-Aided Dispatch and Records Management Systems?

Three shifts are dominating the CAD/RMS space: integration, migration to the cloud, and mobility.

Integration and Interoperability

CAD and RMS systems often have been delivered as integrated suites, with vendors emphasizing seamless data-sharing across platforms. Correspondingly,

integration with other systems can be as important to meet ever-expanding operational needs, especially aggregated data feeds into CAD systems.

Today, telecommunicators must navigate multiple screens — e.g., sensor data, alarms, video, IoT[1] feeds — each siloed and difficult to interpret quickly. The envisioned solution is a backend CAD-embedded aggregation platform that ingests and standardizes data, automatically parsing and presenting only the relevant elements to telecommunicators.

However, though technically feasible, adoption depends heavily on industry-wide data standards and CAD vendors agreeing to support interoperability. Some legacy CAD platforms may require full replacement to enable this capability, whereas newer platforms built on modern software architectures more readily can accommodate standards-based integration. These challenges might be offset somewhat by the ability to leverage AI to digitize millions of records, not merely scanning them but to extract, cleanse, and structure data. Several pilot projects are underway to test the concept.

Cloud Migration Supports Redundancy, Cybersecurity, Scalability and More

Meanwhile, large CAD system vendors are adopting cloud-hosted architectures, following a path previously established by RMS vendors. Cybersecurity is a key driver behind the move to the cloud. Public-safety agencies generally recognize that their internal IT teams cannot keep pace with thwarting security threats or match the security investments made by major cloud providers such as Amazon Web Services and Microsoft Azure. High-profile cyberattacks against public-safety agencies have reinforced this mindset.

Other cloud advantages include scalability, improved disaster recovery, and geo-redundancy, with mirrored data centers making fail-over across regions possible. However, resilient, redundant connectivity is vital when leveraging cloud-hosted systems, i.e., agencies must maintain redundant network paths via multiple commercial carriers, LTE[2] providers, or satellite solutions such as Starlink. If they don't, and a cloud provider suffers an outage — which occurred last year — platforms and over-the-top applications become inaccessible and operations are disrupted, which can be disastrous in the public safety sector, especially the 911 community.

A disadvantage is that cloud technology still is somewhat immature. Another concern regarding cloud-hosted CAD/RMS involves latency, which has improved somewhat but still does not always meet standards-based mission-critical performance levels. Other concerns include a perceived loss of control over data, fees to offload data from the cloud, and long-term subscription costs.

Mobility Improvements for Better In-Field Use

Beyond cloud migration, another major area of recent evolution is mobility. Agencies increasingly deploy smartphones, tablets, and other small-form-factor devices to emergency responders, enabling them to access CAD and RMS functions in the

1 Internet of Things.
2 Long-Term Evolution.

field. Native mobile apps — rather than browser-based interfaces — provide richer functionality and better performance for queries, mapping, and the bidirectional transfer of real-time operational data.

How is Call-Handling Equipment Evolving in Public Safety?

The decline of user group meetings, once valuable for sharing knowledge and best practices, has further limited understanding of CHE capabilities. Consequently, many jurisdictions mistakenly believe that their CHE lacks certain features — often due to limited vendor engagement or insufficient training — and consider switching vendors unnecessarily.

A significant debate is underway concerning native CHE capabilities versus over-the-top applications. The latter tools offer substantial value but are challenging to integrate universally due to the diversity of CAD systems and application programming interfaces (APIs). Over-the-top tools also increase screen clutter and cognitive load for telecommunicators.

As with most aspects of the public-safety environment, artificial intelligence is an emerging opportunity, especially for call triage, translation, transcription, and identifying duplicate or repeat calls. Adoption is slow, however, due to concerns about reliability and fear of being early adopters.

Another major theme concerns the growing shift toward cloud-based CHE, driven by improved reliability, redundancy, scalability, and reduced responsibility for local infrastructure. However, cloud adoption is constrained in regions lacking reliable or diverse connectivity — particularly rural or mountainous areas. Agencies must ensure redundant network paths and understand cloud options and risks.

Looking ahead, four key trends to contemplate are AI integration, cloud migration, shared regional systems to reduce costs, and the ongoing need for agencies to stay current and informed to avoid misinformed or risky upgrade decisions.

How Are Unmanned Aerial Vehicles (Drones) Changing Emergency Response?

Drones are transforming emergency response, and more than 50 public-safety use cases have emerged. The fastest-growing trend is "Drones as First Responder" (DFR) — i.e., automated or semi-automated launches from rooftops that allow drones to arrive before law-enforcement personnel. In 25 percent of calls, drones have determined that no ground response is needed, returning units to service and saving thousands of staff hours.

Drones as First Responder: Use Cases

Two cases in Chula Vista, California, illustrate the life-saving results of this concept. In one, a 911 caller indicated that a man was waving a gun in a public area; however, a drone identified a lighter in the shape of a gun, deescalating the incident and likely preventing a fatal shooting.

In another, a drone located a burning vehicle on Interstate 5. Victims still were in the car and the video feed indicated that the fire was accelerating. Fire department apparatus was too far away, so the information was shared with the California

Highway Patrol, which has jurisdiction over the state's freeways; two nearby troopers pulled the victims out of the vehicle seconds before flashover.

Drones Deliver Emergency Supplies

One of the most interesting emerging use cases concerns using drones to deliver blood products to emergency scenes, a potentially life-saving capability for rural or hard-to-reach locations. Drones already are being used in wildfire fighting to deliver supplies and heavy equipment, preventing personnel from carrying these items long distances over heavy terrain. Blood is difficult to manage in field settings, so drone delivery offers the possibility of dramatically reducing time to transfusion. Pilot programs have demonstrated that long-range, controlled drone delivery is already feasible. The approach also enables interhospital sharing of scarce blood supplies during mass-casualty incidents, with drones parachuting or landing payloads safely at predetermined sites.

Streamlined Drone Waiver Process

Arguably, the most important development is the streamlining of the Federal Aviation Administration's drone waiver process. Public-safety agencies needed special approvals to operate beyond visual line of sight (BVLOS) and to launch drones remotely from rooftops without a dedicated onsite observer. These waivers were extremely difficult and time-consuming to obtain, limiting adoption nationwide.

For six years, the FAA approved only 50 DFR waivers, averaging fewer than 10 per year. Each application required:

- 30–40 pages of technical documentation.
- A visual observer stationed on rooftops during every drone flight.
- Detailed analysis of proposed sensor technologies.
- Complex safety cases addressing collision avoidance and airspace risks.

The lengthy documentation requirements and lack of standardized application procedures created massive delays and inconsistencies. Agencies often waited nearly 11 months for approval.

Over the past year, however, the FAA, influenced by advocacy from the Drone Responders Working Group, adopted a unified waiver template that includes only the essential safety attestations and operational details. The results are eye-opening — 600 waiver approvals in five months, with the average wait time dropping to less than a week.