BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	**)**	
	)	
Modernizing the 911 Framework	**)**	**PS Docket No. 26-197**
	)	**FCC 26-63**
To: The Federal Communications Commission	**)**	

COMMENTS OF
MISSION CRITICAL PARTNERS, LLC

Mission Critical Partners, LLC (MCP) respectfully submits these comments in response to the Notice of Inquiry (NOI) in the above-captioned proceeding. MCP supports the Commission's comprehensive examination of its 911 framework as emergency communications become more Internet Protocol (IP)-based, data-driven, and dependent on a wider range of devices, platforms, networks, and services. The Commission should modernize its scope criteria and harmonize minimum requirements across technologies, while ensuring that new capabilities enter the 911 ecosystem through reliable, interoperable, secure, and operationally governable pathways.

MCP's principal recommendation is that the Commission establish a phased national 911 framework that accommodates evolving technologies, including non-human-initiated emergency communications and data. That framework should distinguish a person's request for help from a machine-generated contact or unsolicited data delivery. It should ensure that devices, applications, platforms, sensors, and artificial intelligence (AI) systems that originate, interpret, transform, prioritize, or transmit emergency communications do not unilaterally impose untested traffic, data, risk, or cost on public-safety agencies. The framework should be national and

technology-neutral, but it must preserve the authority of the appropriate state, territorial, tribal, regional, or local 911 authority to manage deployment and operational use in its environment.

I. Mission Critical Partners

MCP is a professional-services firm that helps public-safety clients enhance and evolve emergency communications systems and operations. Its clients include state and regional 911 program authorities, emergency communications centers (ECCs) — also known public safety answering points (PSAPs) or 911 centers — in nearly all 50 states and the District of Columbia. With more than 200 employees — including former public-safety professionals who have held leadership positions, particularly in the 911 community — MCP brings experience in developing Next Generation 911 (NG911) standards and planning, procuring, implementing, and managing NG911 systems. MCP offers these comments from the receiving-agency perspective, and specifically how emergency communications and associated data can be safely and effectively used by the people and systems responsible for coordinating a response.

MCP's perspective is consistent with its prior Commission filings. MCP has long supported standards-based innovation, public-safety-grade delivery, accurate location and routing, end-to-end interoperability, thorough testing, and clear accountability for entities that interact with the 911 system. MCP also has cautioned that technical capability alone does not establish operational readiness or usefulness. The Commission's modernized framework should build on those principles.

II. Core Objectives and Operational Readiness

The NOI identifies three core objectives that continue to provide a sound basis for 911 policy:

- Ensure public access to reliable, resilient, accessible, secure, and consistent 911 communications across platforms in a way that meets evolving consumer expectations.
- Support public-safety authorities in receiving emergency communications and related information needed to deliver timely and effective emergency services.
- Promote innovative and improved emergency communications technologies regardless of platform, while accounting for feasibility and implementation burdens.

MCP recommends supplementing these objectives with an express requirement that emergency communications and related information be operationally manageable, actionable, and governable by the receiving 911 authority. The ability to receive information does not establish that telecommunicators and responders can identify, understand, prioritize, and act on it safely and promptly.

The Commission should therefore recognize that an NG911 interface capable of receiving data is not blanket consent to receive every data type, at any volume, from every source. NG911 must not become an unrestricted public application-programming interface (API) into operational emergency communications environments. Data must have a defined purpose, an identifiable source, an appropriate delivery method, a recipient capable of using it, and safeguards against unnecessary workload or harm.

This principle does not diminish a person's ability to seek emergency help. A person who needs assistance should not be delayed in receiving it because a technology provider has not completed a new data-integration process. The issue is different when a device, sensor, platform, or algorithm decides that an event is an emergency, sends an alert without a person's active request, or pushes supplemental data to a public-safety entity. The Commission's framework should govern that separate form of ingress.

The NOI already identifies the relevant policy problem. It acknowledges that connected vehicles, wearables, security devices, and other Internet of Things (IoT) technologies can initiate emergency communications without a citizen pressing send. It also acknowledges that automatically generated alarms can save lives but also can consume substantial public-safety time and resources when false. The question now is not merely whether these communications are possible. Rather, it is who determines whether, how, and under what operational conditions they enter a 911 environment.

III. Scope Criteria and Minimum Functional Requirements

The Commission's 911 scope criteria were developed more than two decades ago to identify the services and devices to which Enhanced 911 (E911) rules should apply. The 2003 E911 Scope Order proposed considering real-time, two-way voice service interconnected to the public switched telephone network (PSTN); reasonable citizen expectations of 911 access; competition with traditional commercial mobile radio service (CMRS) or wireline local exchange service; and technical and operational feasibility.[1]

MCP recommends replacing the legacy scope analysis with a function- and impact-based approach. The controlling question should be whether a service, device, or platform enables a request for emergency assistance or materially affects the information, routing, delivery, reliability, or response associated with that request. Real-time voice, PSTN interconnection, and competition with traditional telephone service may remain relevant evidence, but they should no longer be gatekeeping tests in a data-driven environment.

1 *Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems et al*., CC Docket No. 94-102 et al., Report and Order and Second Further Notice of Proposed Rulemaking, 18 FCC Rcd at 25347, para. 18, https://docs.fcc.gov/public/attachments/FCC-03-290A1.pdf

NG911 supports multimedia communications over IP networks and nontraditional access methods, including Next Generation Advanced Automatic Crash Notification (NG-AACN) calls from vehicles, over-the-top (OTT) delivery of emergency location, and requests initiated by IoT devices. The Commission should expand its criteria beyond voice and text to address video, images, and other multimedia, as well as non-interactive or data-only calls. The work of the Communications, Security, Reliability, and Interoperability Council X (CSRIC X) Working Group 5 — which is focused on "Expanding NG911's Multimedia Availability and Increasing 911 Accessibility" — may provide a basis for addressing multimedia availability in an NG911 environment.

The National Emergency Number Association's NENA i3 Standard for Next Generation 9-1-1 (NENA-STA-010.3f) describes non-interactive or data-only emergency calls as automatically initiated calls that carry data, may not be associated with a person, and do not establish two-way interactive media sessions. Examples include burglar alarms, automatically detected hazardous material (hazmat) spills, and flooding sensors. Increasing traffic from sensors, connected devices, and applications could add burdens for public-safety agencies already facing staffing shortages. Including these communications within the framework would provide structure for their delivery and processing.

MCP does not recommend that every technology capable of communication automatically be subject to identical 911 obligations. Rather, the Commission should distinguish among at least four categories:

- Human-initiated emergency communications, where a person actively requests emergency assistance.
- Device-assisted communications with human confirmation, whereby a device detects a potential event, but the user confirms or meaningfully participates in the request for help.

- Fully automated emergency communications, whereby a device, application, platform, or algorithm contacts emergency services without a contemporaneous human request.
- Supplemental or unsolicited emergency data, e.g., information that is sent to a public-safety entity independent of a telecommunicator's request or is beyond the data necessary to establish a communication and route it correctly.

The last two categories warrant particular attention. They may provide valuable help in circumstances involving incapacitation or danger, but they also shift decisions from the person seeking help and the responding public-safety authority to a technology provider's device logic, data source, and release-management process. The Commission should consider source provenance, trigger logic, false-positive and false-negative performance, routing integrity, ability to recontact or cancel, security, and downstream operational impact when it determines whether and how to apply 911 requirements.

For these reasons, competition with traditional voice service should receive reduced weight. A data-driven, specialized, or non-PSTN offering can materially affect 911 service without competing with legacy telephony. Citizen expectations remain important, but they should not be dispositive. Marketing, device design, and public familiarity can create an expectation that help is available even where the technology cannot reliably provide the attributes that public safety needs. The Commission also should consider the reasonable expectations of 911 authorities, telecommunicators, and emergency responders, as the NOI expressly asks.

The Commission should apply a common functional basis for use by services and providers that enable 911 access, independent of the technology used for call or data delivery. Automatic delivery of callback information to reach disconnected callers and location information suitable for routing to the appropriate 911 authority and dispatching responders remain essential. Any entity that provides location information for ECC/PSAP/911 center use should be subject to

comparable requirements for location type, accuracy, and, where appropriate, validation, whether the information accompanies a 911 call or arrives outside the emergency call path.

The functional basis should address source identity, delivery status and failure handling, data provenance, security and authentication, and logging sufficient for troubleshooting and post-incident reconstruction. Requirements should include a callback or recontact capability appropriate for the communication type. Harmonization should retain tailored service profiles for technologies that create additional uncertainty, false-alert risk, data-volume burden, or loss of human context.

The Commission should make clear that voice-centric regulatory classifications cannot be the sole determinant of responsibilities for entities that materially control emergency access, routing, delivery, or data. Operating systems, devices, applications, data platforms, cloud services, and algorithms can perform functions critical to the reliability of the emergency communications pathway.

IV. Phased National Framework for Automated Communications and Data

MCP recommends a phased national framework rather than immediate one-size-fits-all requirements. The framework should create a durable pathway through which new automated technologies can support public safety without requiring every state or locality to reinvent its own technical, operational, and governance process. It should build on recognized standards where they exist, allow for adoption of periodic improvements of those standards, and leave room for development where they do not.

Phase One: National Taxonomy Standards and Qualification

The Commission should work with public-safety agencies, standards bodies, service providers, device and application developers, accessibility advocates, and other stakeholders to

establish a common taxonomy and baseline service profiles. The framework should identify the difference between a human-generated request for help, a machine-detected event, a device-generated alert, and unsolicited supplemental data. It should specify the minimum information that accompanies each category and the conditions under which a category may be delivered to a 911 system.

For fully automated communications and unsolicited emergency data, the baseline service profile should include, at a minimum:

- A clear indicator of whether the communication was initiated by a person, a device, or an automated system, and whether a person confirmed it.
- Source, device or platform class, event type, timestamp, and a way to identify the applicable software or service release for troubleshooting.
- Location source, location timestamp, stated uncertainty or confidence level where available, and an indication of whether location has been modified, inferred, or selected by a user.
- A reliable recontact, cancellation, correction, and update mechanism suitable for the communication type.
- Data provenance that distinguishes raw observations, device-generated values, and AI-derived interpretations or summaries.
- Routing that respects the appropriate public-safety jurisdiction and does not bypass the 911 authority's established dispatch and coordination functions.
- Security, authentication, integrity, logging, and incident-notification practices proportionate to the risk of the traffic or data.

Before broad deployment, providers of higher-risk machine-initiated communications should demonstrate conformance with applicable standards and meaningful end-to-end testing. The

Commission need not decide in this NOI whether every category requires a formal pre-market certification, a recurring certification, a testbed, or another validation mechanism. It should, however, establish the principle that a technology's ability to transmit is not sufficient proof that it is safe to introduce it into operational 911 systems.

Phase Two: Authority-Coordinated Deployment

A qualified service profile then should be deployed in coordination with the appropriate 911 authority. The operational point of control may be an individual ECC/PSAP/911 center, but the governing decision may appropriately sit with a state, territorial, tribal, regional, or local 911 authority, depending on the system architecture and applicable law. The framework should not assume that thousands of individual ECCs/PSAPs/911 centers must evaluate every device or data service independently. Rather, it should permit aggregation and consistency while preserving the ability to manage local operational conditions.

Further, receiving authorities should have reasonable tools to enable, phase, filter, prioritize, pause, or otherwise manage a new category of automated traffic or data. Those controls should be implemented through transparent, standards-based policies and should not be used to block a person's direct effort to summon help. They are necessary, however, to prevent a new service release or data source from unexpectedly overwhelming call-taking operations, creating unsafe cognitive load, or introducing information that cannot be validated or acted upon.

Federal action should complement state, territorial, tribal, regional, and local public-safety governance. National baseline obligations and interoperability expectations should preserve the receiving authority’s role in operational policy, service-profile deployment, and management of the emergency communications environment serving its jurisdiction.

Phase Three: Measurement Feedback and Change Management

The framework should require a practical national feedback loop. Today, a telecommunicator or 911 authority may have no consistent mechanism to report an erroneous, duplicate, false, or operationally harmful automated alert to the entity that generated it. The Commission should seek comment on a standard reporting and remediation path that lets public-safety agencies and their personnel report event-specific problems and lets providers measure and address false activations, misrouting, duplicative traffic, unavailable recontact, and other failures.

Providers also should be subject to disciplined change management. A material change to an emergency-alert algorithm, data type, delivery volume, routing method, security architecture, interface, or software behavior can be distributed widely in a short period. Public-safety agencies need advance notice where practicable, regression and interoperability testing, documented fallback behavior, and a method to contact the responsible provider when operational harm occurs. The need for this discipline continues after a solution's initial deployment.

V. Artificial Intelligence Safeguards

MCP recommends that the Commission distinguish between AI used by a 911 authority within its own operations and AI used upstream of the public-safety sector to initiate, interpret, transform, prioritize, or transmit an emergency communication. These uses create different risks and demand different safeguards and thus should not be treated as a single regulatory category.

Public-safety agencies may use AI-enabled tools for functions such as transcription, translation, quality assurance, analytics, knowledge retrieval, workflow assistance, and decision support. Those uses can improve access and operational effectiveness when implemented responsibly. The Commission should avoid a one-size-fits-all federal prescription for local

operational tools, which must account for local governance, labor, procurement, records, cybersecurity, and response practices. The Commission nevertheless can promote sound principles for all such tools, including human accountability, data security, testing, auditability, accessibility, and clear procedures for identifying and correcting errors.

AI used upstream of the 911 ecosystem presents a distinct concern. An AI system may infer that an emergency exists, determine that a user's words or sensor data merit escalation, create a summary or translation, classify the severity of an event, or determine what information to transmit. In those circumstances, the receiving 911 authority must be able to understand what it is receiving. At minimum, the communication should: identify whether the content is original human communication, device-generated data, an automated classification, or AI-generated interpretation; identify the relevant source and time; and preserve sufficient information for authorized post-incident review.

The Commission should not allow AI-generated certainty to obscure uncertainty in the underlying information. An AI summary, priority score, or conclusion must not be indistinguishable from a caller's statement or verified public-safety information. Providers should evaluate performance for model drift and bias, as well as false positives, false negatives, accuracy, accessibility, language, geographic conditions, and other context relevant to emergency response. They should maintain incident logging, a process for correction and remediation, and change-management controls when a model, data source, or decision rule materially changes. These safeguards are especially important when an AI system can generate traffic to a 911 system without a contemporaneous human request.

VI. Feasibility and Receiving Agency Readiness

MCP recommends that feasibility be assessed across the complete emergency communications lifecycle. An originating platform's technical ability to send data does not

establish that an ECC/PSAP/911 center can receive, display, interpret, record, secure, retain, share, and act on that data without unacceptable risk or cost. The receiving environment is part of the technology's feasibility, not an externality for a public-safety agency to absorb.

The Commission should evaluate, among other factors, call-taking workflow, computer-aided dispatch (CAD) and mapping integration, recording and logging, information display, interoperability, jurisdictional transfer, staffing, training, quality assurance, cybersecurity, data retention, accessibility, procurement lead times, vendor-management obligations, and ongoing support. MCP's prior NG911 implementation work demonstrates why this matters. Data can be forwarded from an originating provider and yet remain unusable because a downstream function cannot process it. A component described as NG911-capable also might require additional modules, patches, interfaces, or configuration before it performs the promised function. The Commission should leverage functional, end-to-end readiness rather than marketing labels or theoretical capability.

The Commission also should recognize differing levels of public-safety readiness. A phased framework should not require that every ECC/PSAP/911 center in a state or region reach identical maturity before an NG911 system can advance. At the same time, an agency's general transition to NG911 should not be treated as a blanket acceptance of all future data and automated-contact types. Readiness must be evaluated for the relevant service profile, data type, workflow, and receiving authority.

VII. Cost Responsibility

The NOI correctly recognizes that feasibility includes implementation burdens. MCP urges the Commission to make clear that parties introducing or enabling a new emergency-communications capability should not transfer its costs to 911 authorities by default. The appropriate neutral baseline is that the upstream ecosystem bears the cost of originating,

complying with the applicable framework, transporting, and delivering its emergency communications and required data to the delivery point designated by the 911 authority. Cost recovery from a 911 authority should not be presumed and should occur only where it is expressly supported by applicable state law or regulation.

This principle is particularly important for automated communications and data. The cost is not limited to connectivity. It includes interface implementation, integration, equipment and software changes, cybersecurity assessments, testing, training, standard operating procedures development, data retention, quality assurance, incident management, and lifecycle support. A national framework that permits new entrants to externalize these costs to public-safety agencies would slow NG911 progress and create unequal access among jurisdictions with different resources.

VIII. Conclusion

MCP urges the Commission to retain the core objectives of its 911 framework, add operational readiness as an express objective, and modernize its scope criteria around function and impact. Consistent minimum requirements, including automatic callback and location information, should apply across technologies, with tailored safeguards for automated communications and unsolicited data. A phased national framework should provide standards, testing, coordinated deployment, feedback, and accountability while preserving reliable human access to emergency response and the operational authority of the public-safety agencies responsible for responding.

Respectfully submitted,

Mission Critical Partners, LLC

By: /s/ *John Chiaramonte*
John Chiaramonte, ENP, PMP
President, Enterprise AI Strategy
Mission Critical Partners, LLC
690 Gray's Woods Blvd
Port Matilda, PA 16870
888.862.7911

Date: November 16, 2026