

Broadband First

A Strategic Investment Framework for Public Safety Communications

Field observations and a network centered framework from MACC911, Grant County, Washington

"Connectivity is the new electricity." The next communications architecture should treat it that way.

Brent VanKeulen Deputy Chief (Ret.), Western Fire Chiefs Association

D.T. Donaldson Director, MACC911

Gerrit A. Klein Technical Services Manager, MACC911

A NOTE ON VENDOR REFERENCES

This paper identifies specific products when necessary to describe the equipment used in the field demonstration. Product references document the test configuration and do not imply endorsement.

Table of Contents

	Executive Summary	1
	Background	5
SECTION 1	The Field Experiment	7
SECTION 2	The Question It Raised	8
SECTION 3	What Has Actually Changed	10
SECTION 4	From an LMR-Centered Model to a Network-Centered Model	12
SECTION 5	From Push to Talk to Push to Know	16
SECTION 6	Resilience Over Redundancy	18
SECTION 7	The Economics	19
SECTION 8	Standards and Vendor Independence	23
SECTION 9	Interoperability Beyond the LMR Footprint, and What Leaders Should Do Now	26
SECTION 10	Conclusion	29
APPENDIX A	The Field Test in Detail	30
APPENDIX B	A Practical Migration and Investment Plan	38
APPENDIX C	Glossary	45
	Acknowledgments	47
	Sources and Method Notes	49
	About the Authors	50

Executive Summary

For 911 directors, police chiefs, and fire chiefs: there is a more strategic way for agencies to invest in public safety communications, one that can deliver resiliency and greater capabilities at lower cost.

In August 2026, the Multi Agency Communications Center (MACC911) in Grant County, Washington, hosted a field test that challenged assumptions about how public safety agencies should invest in communications infrastructure. The field test showed that public safety leaders can best serve their responders and communities by organizing public safety communications around resilient broadband networks rather than around a single technology, their radio system, as many agencies do today.

This reframed approach, where the radio system is no longer viewed as the public safety communications network but rather as part of it, improves decision-making and can lead to greater capabilities at lower cost. Though the outcomes may ultimately prove transformative, this practical approach can be implemented prudently and incrementally, starting at a low financial entry point that does not require a bond measure or procurement cycle.

Nothing here calls for taking radios from firefighters or police officers. The radio system public safety agencies have long relied upon, land mobile radio (LMR), remains extraordinarily good at immediate shared tactical voice communications. Agencies should keep these systems healthy and continue funding them for that purpose. In fact, LMR can be even more effective when it is one component of a broadband-centered network. The first step is to put the radios you already own on the internet.

What the field test showed

More than 60 public safety professionals gathered in central Washington to answer three practical questions about interoperability:

- How quickly could four agencies running different, unconnected radio systems across three states, Washington, California, and New Mexico, communicate with one another using broadband infrastructure?

- Once network paths serving the different agencies are connected through a blended broadband architecture, how would the infrastructure perform when the paths are removed one at a time during live radio traffic?
- How effective is a public safety vehicle, equipped with a gateway, at serving as a communications node between LMR and broadband? Chiefly, how far could a vehicle extend radio coverage?

The answers came by afternoon. The disparate systems could talk to one another. A continuous radio transmission, a common talkgroup, remained connected while cellular and satellite network paths disconnected one at a time. A vehicle-based gateway enabled an officer to stay connected on his radio while in a cellular dead zone inside a jail. Separately, a vehicle-based gateway supported portable radio communications up to 4.7 miles away.

As a result, the exercise soon moved beyond questions of interoperability to a question about architecture: if a temporary field setup can do this, what exactly are agencies buying when they spend tens of millions of dollars on traditional radio infrastructure? That question may sound provocative, so it is worth stating plainly that agencies are buying a capability that has saved lives for decades.

The demonstration did, however, identify assumptions that agencies should examine before committing long-term capital to a communications architecture. Agencies should not invest new capital in their radio systems by default. They should instead direct funding to the option that best meets their requirements for operational capability, resilience, coverage, and future flexibility. Sometimes investment in LMR will be the right choice, but that should be proven relative to other options instead of assumed.

Field test limitations and open questions

The exercise in August was a field test, not a controlled or longitudinal study.

Alongside successes, the team observed issues including intermittent audio loss in some situations, differences in emergency button behavior among systems, and restrictions on mobile radio transmission while certain gateway configurations were active. These issues affect operational readiness and require controlled testing. Agencies evaluating this architecture should address each issue before deployment.

The paper's Appendix A reports these failures in the same level of detail as the successes because that is the information most useful to an agency planning its own test.

Cost comparisons

Existing radio systems enter every budget discussion with a built-in advantage: they already exist. Agencies extend life, replace aging components, add sites, renew support, and modernize backhaul because each individual step looks smaller and safer than reconsidering the architecture.

A full LMR system replacement in the western United States now runs \$25 million to \$50 million. A single new tower site costs \$2 million to \$3 million. Equipping one patrol or fire vehicle the traditional way, with a mobile radio, portable, and repeater, can run \$20,000 to \$25,000.

In contrast, a resilient broadband package for a single public safety vehicle, served by multiple cellular carriers and satellite, can run roughly \$10,000, which is about half the traditional radio buildout. At that order of magnitude, \$1 million can equip roughly 100 vehicles with resilient broadband. Those vehicles can then support voice, computer-aided dispatch (CAD), video, location, messaging, remote access, and future applications.

In many settings this is a direct substitute for a tower. A vehicle fleet carrying blended broadband and radio gateways can deliver communications across the same service area as a proposed tower at a fraction of the capital cost, while adding data capabilities the tower cannot provide.

In narrow cases, however, a tower may be the right choice, with coverage that persists whether or not a vehicle is nearby, engineered to a defined reliability standard across a defined footprint, and with performance that does not depend on commercial network availability.

This supports the case that agencies should evaluate radio alongside its alternatives, with radio competing for the same dollar rather than receiving it automatically.

A low-cost entry point

Even small agencies with tight budgets should be able to test the claims in this paper. The starting point can be a single radio the agency already owns, a gateway device, and a commercial push-to-talk application, a combination that can be assembled and tested for under \$5,000. A chief, director, or technical services manager can form a first-hand judgment within a month about whether the architecture holds up under their own operating conditions, with their own dispatchers and field personnel, before any larger decision is made.

Most agencies find that the core function works better than expected, and the operational details around it need more attention than expected. Both are useful discoveries and worth having early.

A practical migration and investment plan

Most agencies will face a major radio system decision within the next five years. Whatever architecture they specify tends to get locked in well before the system goes live, and stays locked in for the next two decades. An agency that writes its next specification around the system it currently owns will get a newer version of that system, then discover afterward that the capabilities it wanted must be purchased separately, on top, at additional cost.

A broadband-centric strategy does not mean replacing the radio system tomorrow, abandoning infrastructure that works, or betting the agency on one carrier, one vendor, or one new technology. The practical approach is simple. Keep the existing LMR system in service. Start building a resilient broadband layer alongside it. Move capabilities to that layer when there is a clear, operational reason. Measure the results. If it works, expand it. If it does not, fix it before spending the next dollar.

Appendix B lays out a phased, five-year investment plan built on that sequence, with rough order-of-magnitude figures for each stage and a procurement checklist. For a mid-sized regional agency, the total cost estimate is roughly \$1.3 million to \$2 million, with each phase proving itself before the next begins.

Define success at the responder level

The final measure of a communications system is not simply whether it works but whether it works for the responder. It should be designed and tested under real-world conditions. The paper outlines questions to evaluate whether a system will be acceptable to responders. Most importantly, do they trust the system enough to use it during an actual emergency?

The bottom line

Advancements in technology give public safety leaders the opportunity to better support their responders in the field with greater capabilities at lower cost. By organizing public safety communications around resilient broadband networks, rather than a single technology, they can help responders carry out their critical missions and save lives. The paper urges leaders to consider these findings and suggestions, conduct their own economical tests, and form their own opinions. When the decision is to move forward with a broadband-centric network, this paper provides a judicious, phased plan to help guide the transition.

Background

In August 2026, MACC911 brought more than sixty public safety professionals to central Washington to test how quickly agencies using different radio systems could communicate and how a blended broadband architecture would perform as individual network paths were removed. The team also tested communications beyond the trunked LMR coverage area. Portable radios operating in direct mode connected to vehicle mounted radios in gateway mode, which then carried voice traffic over broadband to the participating systems.

Four trunked LMR systems in three states operated on a common talkgroup. Two systems that had no previous connection to MACC joined the talkgroup during the exercise in approximately ten to fifteen minutes each. All radio traffic traveled over gateway and broadband connections. A responder in Grant County communicated with a responder hundreds of miles away using each agency's normal portable radio, without reprogramming either radio. A continuous transmission remained connected as Verizon, FirstNet, AT&T, T Mobile, and Starlink paths were removed one at a time. A deputy also maintained voice communications in a jail area with no usable cellular service nor access to the trunked LMR system by using a vehicle gateway. During a separate range test, portable radio communications reached approximately 4.7 miles from the vehicle in direct mode and back to the dispatch center and all four trunked systems.

A battalion chief who initially questioned the need for broadband and gateways left the demonstration asking whether the approach could support routine operations.

This paper takes that question seriously. The argument is straightforward. Public safety communications should be organized around resilient connectivity rather than around the radio system. LMR should remain where it is strongest, particularly immediate shared tactical voice, and become one component of a broader communications architecture rather than the architecture around which every other capability is built.

The radio system should no longer be the public safety communications network. It should be part of the public safety communications network.

That reframing changes the investment question more than it changes the technology. A new LMR tower site runs two to three million dollars. Full LMR system replacements in the western region have come in between twenty five and fifty million. Equipping a single vehicle the traditional way, with a P25 mobile, a portable, and a vehicle repeater, can run twenty to twenty five thousand dollars. At roughly ten thousand dollars per vehicle, one million dollars equips about a hundred public safety vehicles with blended broadband that carries voice, CAD, video, location, and messaging rather than one modality. In many settings that is a direct substitute for a tower and belongs in the same column of the same spreadsheet. Sometimes the tower still wins. It should have to prove it.

Nothing here argues for removing radios from firefighters or police officers. Existing LMR should be maintained while it does critical work. The argument is against pouring the next generation of capital into it by default.

The field demonstration also identified limitations. Emergency alarm data did not cross the gateway in every configuration. Audio returning through the Inter RF Subsystem Interface to the dispatch trunk dropped intermittently. Personnel could not transmit on a mobile radio while that radio was operating as the gateway. These unresolved issues require controlled testing before operational use.

The practical entry point is smaller than most leaders expect. For a few thousand dollars, using a radio the agency already owns, a low cost gateway, and an off-the-shelf push-to-talk application, a chief or director can put one talkgroup on the network and form a first-hand opinion within a month, with no bond measure and no procurement cycle. That matters most to small agencies and tight budgets, where the cost of finding out has been the barrier. Most agencies discover that the core function works better than expected and that the operational details around it need more attention than expected. Both findings are worth having early.

Many agencies will face a major radio system decision within the next several years. Because specifications establish the architecture before implementation, agencies should evaluate broadband, LMR, and interoperability requirements before issuing a solicitation.

Appendix A documents the field test, including observed failures and open questions. Appendix B presents a phased five year investment plan, planning estimates, and a procurement checklist. Appendix C is a glossary page.

SECTION 1

The Field Experiment

In August 2026, MACC911 brought together more than sixty public safety professionals in central Washington to test communications technologies and practical interoperability. The exercise examined how quickly agencies using different radio systems could communicate, how a blended broadband architecture performed when individual network paths were removed, and how far a portable radio remained usable when a public safety vehicle bridged local RF traffic to broadband.¹

By late afternoon the interesting question had changed. Whether disparate systems could talk to one another was settled. They could. What remained open was whether the architecture we had just assembled pointed toward a different way to build public safety communications in the first place.

What we observed

- Four separate trunked LMR systems operated simultaneously: MACC911, LA County RICS, New Mexico State Police, and Spokane. Spokane and New Mexico each joined the test environment in approximately ten to fifteen minutes through a VM8000 operating in gateway mode and the ESChat platform. Personnel coordinated the configuration by telephone.
- A continuous radio transmission remained connected while Verizon, FirstNet, AT&T, T Mobile, and Starlink paths were removed one at a time.
- A deputy maintained voice communications with dispatch in a jail area with no usable cellular service and no access to the P25 trunked system by using the vehicle gateway.
- During a wildland range test, a portable radio maintained push to talk communications at approximately 4.7 miles from the vehicle.
- Portable radios from multiple manufacturers passed traffic through the Viking mobile gateway.
- A broadband-only talk path operated end to end without LMR infrastructure connecting public safety grade radios and consumer smart phones. Lifeline Ambulance already uses a similar broadband PTT model operationally across multiple counties.

PARTICIPANT OBSERVATION

A battalion chief arrived unsure of the need for the approach. By the end of the day his question had shifted to why the department could not simply operate this way all the time. That is the question this paper takes seriously.

What the day did not prove

This was a field demonstration, not a controlled or longitudinal study.

The team observed intermittent ISSI audio loss, differences in emergency button behavior among systems, and restrictions on mobile radio transmission while certain gateway configurations were active. These issues affect operational readiness and require controlled testing. Agencies evaluating this architecture should address each issue before deployment.

Appendix A documents the full test day: what was configured, what was tested in what order, what passed, what failed, and what we would do differently. Readers who want the evidence behind the summary above should start there.

The demonstration identified assumptions that agencies should examine before committing long term capital to a communications architecture.

SECTION 2

The Question It Raised

If a temporary field setup can do this, what exactly are agencies buying when they spend tens of millions of dollars on traditional radio infrastructure?

The question can sound provocative, so the first answer should be plain. Agencies are buying a capability that has saved lives for decades. Land mobile radio is purpose-built and extraordinarily good at immediate shared voice. A first responder calling a mayday does not need a lecture about convergence. They need the microphone to work.

What deserves scrutiny is whether the entire communications ecosystem should stay organized around LMR because LMR has historically been the most important tool in it.

Public safety communications should be organized around resilient connectivity rather than a single technology. LMR should remain where it performs best, particularly for immediate shared tactical voice, while operating as one component of a broader communications architecture.

This approach changes the investment question. Agencies should direct funding to the option that best meets documented requirements for operational capability, resilience, coverage, and future flexibility.

THE RADIO SYSTEM SHOULD NO LONGER BE THE PUBLIC SAFETY COMMUNICATIONS NETWORK. IT SHOULD BE PART OF THE PUBLIC SAFETY COMMUNICATIONS NETWORK.

Public safety has seen this pattern before. Legacy 911 telephony began as a way to deliver emergency voice calls, but over time its architecture helped determine where call-takers worked, how centers were physically designed, how calls were transferred, how redundancy was engineered, and how responsibilities were divided among carriers, PSAPs, and vendors. NG911 is now unwinding many of those assumptions by separating services and applications from the network and physical location. The broader lesson is that a technology that begins as the essential solution to one problem can gradually become the organizing structure for many adjacent problems. Workflows grow around it. So do procurement specifications, training curricula, staffing models, governance structures, and vocabulary. Eventually the system stops being designed from first principles and starts being designed around what already exists.

The August test separated functions that are often procured together. Voice originated on a portable radio, passed through a vehicle gateway and one or more broadband paths, traversed an Internet Protocol push to talk platform, and reached users and radio systems outside the original RF coverage area. This separation allows agencies to evaluate each architectural layer independently; architecture becomes a design choice rather than a historical inheritance.

SECTION 3

What Has Actually Changed

Broadband can carry voice, data, video, and application traffic that previously required separate communications paths.

Modern public safety broadband supports priority and preemption, mission-critical push-to-talk, location, video, messaging, sensor data, and applications that did not exist when most current LMR architectures were designed. FirstNet's standards work treats mission-critical voice, video, data, HPUE, resiliency, quality of service, priority, preemption, security, and interoperability as parts of one broadband ecosystem.² What that combination makes possible in daily operations is the subject of Section 5.

FirstNet deserves credit for changing the market, and it is worth saying so clearly in a paper that argues for moving away from dedicated public safety infrastructure. The network did more than add a carrier option. It set public-safety-specific expectations for priority, preemption, deployable coverage, devices, and standards-based mission-critical services, and it pushed the commercial market to compete harder for public safety business. Agencies benefit from that competition.

High-power user equipment illustrates the shift. FirstNet describes HPUE as transmitting at up to six times the power of an ordinary cellular device on Band 14, which improves range at the network edge and building penetration in some conditions.³ The usable edge has moved.

Low Earth orbit satellite service adds another access path, with requirements for sky view, power, mounting, network management, and recurring service. Terrestrial cellular and satellite networks have different infrastructure and failure modes, which can improve path diversity.

The vehicle becomes a communications node

MACC has outfitted approximately sixty first-out vehicles with a resilient connectivity package. Each one carries a blended multi-path gateway, multiple cellular subscriptions across different carriers, satellite where the mission justifies it, and vehicle Wi-Fi.

The radio gateway is the newer piece and it is not yet in the fleet. No MACC vehicle carried a VM8000 before the August test. The results of that test are what prompted the agency to begin installing them, and the intent is to equip the fleet over time. Read what follows as a design direction supported by a field demonstration rather than as an installed base.

Once both elements are present, the vehicle stops being a consumer of the communications system and becomes part of its infrastructure.

That fleet design reflects a specific idea. A blended multi-path gateway aggregates several broadband connections into one managed link. It evaluates bandwidth, latency, packet loss, and jitter continuously, then routes traffic at the packet level across whatever connections are healthy. It does not wait for a single active link to fail before switching.

MACC's implementation pairs Dejero GateWay devices running Smart Blending with cellular service including FirstNet and HPUE, additional commercial cellular paths, and Starlink in selected configurations, integrated and supported by IP Access International.⁴ Other bonded-connectivity products and integration partners are available, and the architectural requirement is the behavior rather than the brand.

The design philosophies differ more than the hardware does. Traditional failover asks which connection is primary and what stands behind it. A blended architecture asks which paths are healthy right now and how the application continues while conditions change.

MACC began deploying the blended broadband portion of this configuration before the August test under a plan covering approximately sixty initial response fire, law enforcement, and EMS vehicles. During a wildfire operation, Royal Slope Fire Rescue reported clear broadband communications in areas where the existing P25 coverage was weak or absent, including areas outside Grant County.⁹ This operational report preceded the field demonstration.

Voice can ride the same network

A broadband push-to-talk platform provides the voice layer. It operates on smartphones and purpose-built devices, connects to P25 through ISSI, and connects to other LMR systems through gateway interfaces. Voice stops being bounded by the footprint of a single RF system.

MACC uses ESChat for this layer, and it is the platform that carried voice during the August test.⁵ Several mission-critical push-to-talk platforms offer comparable interconnection, and the strategic requirement is open, manageable interconnection between broadband users, dispatch, P25, and other LMR systems rather than any particular application.

Getting radio traffic onto IP is the first strategic step we would recommend to almost any agency. RF stays where it is. What changes is that voice gains a path beyond RF. Once voice can cross the network, a local talkgroup can extend to a remote dispatcher, a mutual-aid partner, a smartphone, a broadband PTT device, another P25 system, or a radio gateway, and those endpoints no longer have to live inside one traditional radio system.

CONNECTIVITY IS THE NEW ELECTRICITY

Public safety does not build a separate generator for every application that needs power. It builds a resilient electrical system and lets many applications consume it. Connectivity is becoming that kind of utility. The strategic goal is a network layer that phones, CAD, radio, video, sensors, AI, and applications nobody has selected yet can all draw from.

SECTION 4

From an LMR-Centered Model to a Network-Centered Model

Public safety treats the radio system as one conceptual object. Inside it sit several distinct things: the voice application, portable and mobile RF access, tower sites, backhaul, talkgroup management, encryption, console integration, and interoperability. They grew up together, so they get procured and governed together.

IP networking pulls those layers apart. Engineering gets no simpler for it. What changes is that the design choices become visible, which lets leaders ask a better question than whether to replace P25 with broadband.

Which combination of applications, access methods, and transport paths gives us the most resilient communications architecture for the money?

The table below is a conceptual illustration rather than a design specification. Each column holds representative examples, and the point is the separation itself.

APPLICATIONS	ACCESS	TRANSPORT AND BACKHAUL
Voice and PTT	LMR RF	Microwave
Messaging and status	LTE and 5G	Fiber and Ethernet

APPLICATIONS	ACCESS	TRANSPORT AND BACKHAUL
Location and AVL	HPUE and Wi-Fi	Commercial IP
Video and imagery	LEO satellite	Satellite backhaul
CAD, data, AI	Local RF gateway	Private and public cloud paths

Public safety already made this transition once

NG911 is the closest analogy, and Section 2 described how legacy 911 telephony came to shape far more than call delivery. The architectural move is what matters here. NG911 shifted toward standards-based IP networks and Emergency Services IP Networks, separating services and applications from the transport carrying them. NENA's i3 architecture formalizes that separation, making the network the platform on which multiple services operate.⁷

Modern P25 systems already run IP internally, so the question here has nothing to do with analog radio versus the internet. The question is what sits at the center. In an LMR-centric design the radio system remains the organizing structure and IP supports it. In a network-centric design the communications network becomes the organizing structure, while LMR, LTE, satellite, fiber, microwave, Wi-Fi, and gateways become available paths and components.

LMR remains extraordinarily good at the problem it was designed to solve. The strategic mistake is designing the entire public safety communications ecosystem around that one problem.

Interoperability changes shape

Traditional interoperability gets engineered between known systems. This P25 system connects to that P25 system. This patch joins these two channels. This radio cache is programmed for this mutual-aid plan. Those methods still work, and they assume the participants and the geography are known in advance.

A network-centric PTT layer changes the geometry. A user joins from a broadband device. A local radio joins through a gateway. A P25 system joins through ISSI. Another LMR system joins through a different gateway. Their common point becomes the network and the application.

The August test is a concrete illustration. Four trunked radio systems in three states shared a common talkgroup. MACC911 connected through ISSI. Spokane and the New Mexico State Police, neither of which had any prior connection to MACC, were brought onto the talkgroup during the exercise in roughly ten to fifteen minutes each. Only the configuration was handled by telephone. The traffic itself ran over the radios.

What that meant in practice is worth stating plainly. A responder in Grant County keyed the portable radio already on their belt and spoke to a responder six hundred miles away in LA County, who answered on the portable radio already on theirs. Neither radio was reprogrammed. Neither user changed anything about how they normally operate. None of it required a radio cache, a mutual-aid frequency plan, or a bilateral agreement negotiated in advance.

Engineer interoperability all the way to the end user

Interoperability cannot stop at the network. The engineered solution has to begin at the network level and continue all the way down to the firefighter, deputy, EMT, or dispatcher actually trying to communicate during an emergency.

A network engineer can connect multiple systems through ISSI, gateways, broadband PTT, or other interfaces. That is important work, and the technical connection is not the operational outcome. The operational outcome is that Jane Firefighter presses one button and talks to the people she needs to talk to.

If interoperability requires a responder to remember a series of channel changes, switch operating modes, manipulate a gateway, monitor a second device, or recall a procedure used twice a year, assume that eventually it will not happen when it matters. That is not a criticism of the responder. It is a design failure.

Public safety personnel use communications equipment while driving, treating patients, operating apparatus, fighting fire, searching buildings, managing scenes, and physically dealing with offenders. The architecture should reduce their workload. A portable radio interoperability function should therefore come as close to one-button operation as the technology reasonably allows, and the same standard applies to a vehicle gateway. A gateway technically capable of connecting multiple systems but requiring someone on scene to work through menus, configurations, and unfamiliar procedures is unfinished engineering. The work is complete when the user accomplishes the operational objective quickly, predictably, and with minimal thought.

Simplicity at the user level usually requires considerable complexity behind the scenes, and that is an acceptable trade. The responder should not have to understand how many networks, gateways, carriers, interfaces, encryption domains, or applications are involved in establishing a communications path. Those decisions should be engineered, tested, automated, and managed before the emergency. The network can be complicated. The user experience should not be.

The channel plan is part of the architecture

An agency can build the most resilient network in the world and still create poor interoperability through an inconsistent or poorly maintained channel plan.

Talkgroups and channels should be logically organized, intuitively named, and, where practical, consistent across participating agencies and subscriber devices. A responder moving from one radio to another should not have to learn a different communications philosophy. Common operational channels should appear in predictable locations. Naming should make sense to the people using the radios rather than only to the technicians programming them. Mutual-aid and interoperability resources should be easy to find without a laminated cheat sheet during an emergency.

Channel plans, templates, user groups, gateway configurations, permissions, and interoperability procedures also need regular review with the people who actually use them. Systems change. Agencies change. Mutual-aid relationships change. Personnel change. The application layer has to be maintained as deliberately as the network beneath it.

Interoperability therefore has two tests. Can the systems connect? And can the responder use that connection immediately, under stress, without having to think about how it works? A public safety communications architecture has not solved interoperability until the answer to both is yes.

AN IMPORTANT TECHNICAL CAVEAT

A gateway is not a feature-for-feature replacement for a formal ISSI. For many mutual-aid and incident use cases a gateway delivers the function leaders actually care about, which is that users can talk, at dramatically lower cost and setup time. Network-level identity, emergency behavior, encryption, console features, recording, and governance may all behave differently. Test those differences before relying on them.

An open architectural question

During parking lot testing, several vehicle gateways operated near one another, each with independent connectivity. Observers reported no duplicate audio, looping, feedback, or interference. The results were better than expected, but controlled testing is required before broader conclusions can be drawn before broader conclusions can be drawn.

Suppose gateways were placed at fixed radio sites or inbuildings with good antenna systems and solid IP connectivity, and also deployed in vehicles. Could portable radios then operate primarily in conventional direct mode, with the nearest fixed or mobile gateway bridging into the IP

network for wide-area communications? Direct-mode RF would become the local access layer. The microwave and internet backbone would become the resilient infrastructure, carrying LMR voice as one application among several.

A two-day parking lot test proves none of this at scale. What happens when multiple gateways hear the same portable, how duplicate traffic gets handled, how the outbound gateway is selected, and whether there is a practical ceiling on participating gateways are all unresolved. We raise it because it is the natural extension of what we observed and because the industry should be working on it.

SECTION 5

From Push to Talk to Push to Know

Public safety communications is moving from a voice-centric workflow toward an information-centric one. Broadband changes what information can move, when it moves, and who receives it.

A traditional portable radio is superb at one core job: immediate shared voice and, depending on the system, some metadata. A broadband-connected device carries that same voice while also carrying GPS location, text, photographs, live video, CAD information, maps, floor plans, premise data, translation, sensor alerts, automatic status, drone feeds, remote cameras, and whatever data source becomes useful next year.

The dispatcher's role changes with it. With voice alone, a dispatcher hears the unit. With an information-rich network, the same dispatcher hears the unit, knows where it is, sees relevant imagery, receives status automatically, and pushes information to the responder without forcing every fact through a shared audio channel.

What is the radio channel actually carrying?

To pressure-test the assumption that routine operational information belongs on voice, MACC ran an exploratory AI-assisted categorization of 1,000 consecutive law enforcement radio transmissions drawn from a randomly selected continuous period. Roughly one to two percent were categorized as genuinely critical or time-sensitive. About ninety percent or more appeared capable of being handled as well or better through CAD status, GPS and location data, records returns, secure messaging, automated acknowledgements, or other administrative tools.⁶

This is not a peer-reviewed study. A sample from one center is not a national benchmark, and other agencies may find different distributions. It is an operational sample that raises a useful question.

Public safety has confused things that happen to be done over radio with things for which radio is the best medium.

COMMON VOICE TRAFFIC TODAY	POTENTIAL BETTER DEFAULT PATH
En route, arrived, clear, available	CAD status, AVL, geofence or automatic state change
Unit location checks	AVL, breadcrumb, responder location
Routine dispatch details	CAD push, mobile alert, premise notes, map
License and records returns	Mobile data or secure messaging
Administrative coordination	Chat, forms, tasking, phone
BOLO descriptions and images	CAD, text, image broadcast
Fire and EMS benchmarks	CAD timers, buttons, automated prompts
Officer emergency, mayday, pursuit, IDLH	Immediate shared voice remains primary

Moving routine status and database traffic off voice does not make radio less important. It can make radio more valuable. When the channel has stopped serving as a status board, a CAD audit trail, a records terminal, a confirmation system, and an administrative chat room, the remaining traffic carries more signal. Someone keys the microphone and listeners expect there is something worth hearing.

Mayday calls, officer emergencies, pursuits, rapidly changing tactical operations, and IDLH fireground communications stay voice-critical. Broadband data should strengthen those moments. Reserve each medium for the work it performs best.

SECTION 6

Resilience Over Redundancy

Public safety uses redundancy and resilience as synonyms. They are different design ideas. Redundancy usually means a second thing waiting behind the first. Resilience means the mission continues through different paths, modes, locations, and systems while individual components degrade or disappear.

A primary fiber and a backup fiber look redundant. If both share a conduit, a carrier core, a power plant, or an upstream provider, they can fail together. A cellular router with a second SIM looks redundant. If it switches only after the first path becomes unusable, the application still experiences the interruption. Resilient design pays attention to failure domains, and device counts tell you very little.

Packet-level blending is what makes the difference operationally. Rather than ranking connections into a primary and a backup, the gateway uses every healthy path at once and moves traffic between them continuously. The loss of any one path becomes a reduction in available capacity instead of an interruption. The Dejero devices in MACC's fleet operate this way, and several vendors now offer comparable bonding.⁴

None of that supports a claim that a multi-carrier architecture can never fail. Commercial carriers share fiber routes, power dependencies, data centers, weather exposure, and regional congestion. Satellite systems carry their own common-mode risks. Cybersecurity and cloud dependencies add more. The credible claim is narrower and stronger: combining genuinely diverse terrestrial and satellite paths substantially reduces dependence on any single provider, site, backhaul route, or technology.

The vehicle as an edge node

In a rural county, public safety vehicles are already distributed across the service area. Equip them with resilient broadband and a radio gateway and they become mobile communications nodes. The vehicle provides Wi-Fi and IP connectivity to computers and applications, uses multiple carrier and satellite paths to reach the network, and extends a local RF bubble for nearby portables.

The gateway function itself belongs to the radio. During the August test that role was performed by EF Johnson VM8000 mobile radios, with VP8000 portables operating in direct mode to reach

them.¹¹ The bring your own radio result matters here for the same reason it matters to the vendor-independence argument in Section 8. Portables from several manufacturers passed traffic through the same gateway onto the same talkgroup. Comparable gateway capability exists across the industry, and an agency should confirm it in its own fleet rather than assume it.

That is why the 4.7-mile portable-to-vehicle result matters. Terrain, antenna placement, band, power, obstructions, and RF noise still govern range, and no agency should plan on 4.7 miles in every environment. What the result demonstrated is that a vehicle can serve as part of the system's edge infrastructure.

The jail dead-zone test showed the same principle running the other direction. A user entered a location where direct cellular service and trunked LMR disappeared and the communications path continued through the vehicle gateway. Local RF covered one gap. Broadband covered another.

Restoration after infrastructure loss

Recovery changes too. FirstNet maintains deployable assets designed to restore local broadband coverage during disasters and major incidents, including satellite-backed cell sites and airborne options, and those assets can reach an emergency within hours.⁸ A fixed radio tower destroyed by wildfire, ice, or structural failure presents a much harder recovery problem.

Cellular infrastructure is not invulnerable. A network-centric architecture simply gives incident leaders more ways to restore the service. A replacement path can arrive by vehicle, trailer, aircraft, temporary satellite terminal, alternate carrier, or an unaffected neighboring network. Diversity gives operations room to maneuver.

SECTION 7

The Economics

Radio capital planning is hard because the current system carries a powerful advantage into every budget discussion. It already exists. Sunk cost creates gravity. Agencies extend life, replace aging components, add sites, renew support, modernize backhaul, and upgrade encryption because each individual step looks smaller and safer than reconsidering the architecture.

Sometimes that is the right call. Existing LMR infrastructure should be maintained while it provides critical service. The risk is letting maintenance necessity harden into an automatic growth strategy.

The cost of keeping a mature LMR system healthy

MACC's own numbers illustrate the pattern. Its P25 network includes more than a dozen radio sites. In 2025 MACC contracted for approximately \$95,000 per year of senior on-site radio technical support. By spring 2026 multiple site components were at or approaching end of support. RF components were estimated at \$50,000 to \$75,000 per site. DC power systems ran \$75,000 to \$100,000 per site. Six RFSS controllers came in at roughly \$35,000 each. MACC separately authorized approximately \$180,000 for replacement GPS timing units, and that figure excludes installation labor.⁹

Every one of those is a lifecycle cost inside a system that already exists. None of it buys new capability.

Replacement projects become capital programs measured in tens of millions. Clackamas County, Oregon, authorized \$59 million in general-obligation bonds in 2016 to replace an obsolete emergency radio system and expand coverage, and later project documents describe additional site-construction contingency needs.¹⁰

Nothing about those figures is scandalous. Hardened sites, towers, backhaul, power, shelters, engineering, permitting, maintenance, and support cost what they cost. The strategic question is what capability each additional dollar buys relative to the alternatives now available.

The opportunity-cost comparison

MACC's vehicle connectivity deployments give a useful scale reference. A well-equipped vehicle connectivity package, comprising a blended multi-path gateway, antennas, installation, integration, and configuration, has run on the order of \$10,000 per unit in MACC planning, depending on configuration and inclusions.⁹ At that order of magnitude, \$1 million equips roughly one hundred public safety vehicles with resilient broadband. Those vehicles then support voice, CAD, video, location, messaging, remote access, and future applications.

Agencies should build this number for themselves rather than adopt it. Configuration, carrier mix, satellite inclusion, antenna choices, vehicle type, installation labor, and integration all move it, and a competitive procurement across bonding vendors and integrators may move it further. The traditional comparison point is worth having in hand as well. Equipping one vehicle with a P25 mobile, a portable, and a vehicle repeater can run twenty to twenty five thousand dollars.

Upgrade projects deserve the same scrutiny as new construction. Many wide-area radio upgrades now underway are migrations from P25 Phase 1 to Phase 2, which doubles talkgroup efficiency. That upgrade can require new base stations and a large number of new subscriber radios, and what the agency receives for it is additional talkgroup capacity, a capability broadband PTT platforms provide from the day they are turned on. Upgrades costing tens or hundreds of millions of dollars can deliver a great deal to the vendor selling them and comparatively little to the user carrying the radio. That is a question worth asking out loud before the purchase order is signed.

In many settings this is a direct substitute for a tower, and it should be evaluated that way. A vehicle fleet carrying blended broadband and radio gateways can deliver usable communications across the same service area a proposed tower was meant to cover, at a fraction of the capital cost, while adding data capabilities the tower could never provide. Agencies weighing a coverage gap should put both options in the same column of the same spreadsheet.

Where the tower still wins is narrow and worth naming precisely. Fixed-site RF delivers coverage that persists whether or not a vehicle is nearby, engineered to a defined reliability standard across a defined footprint, with performance that does not depend on commercial network availability. Those attributes matter in specific circumstances. They do not justify treating every coverage problem as a tower problem.

Where the next dollar goes

The business case is less about finding an entirely new pot of money than about changing where the next communications dollar lands.

Broadband First does not mean an agency stops maintaining LMR. A healthy P25 system should stay healthy. It is doing an extremely important job, particularly for immediate tactical voice. The change belongs in new capital investment and system expansion.

When the next project is another tower, another proprietary interface, a major RF expansion, or a large subscriber refresh, that project should stop getting funded automatically because it belongs to the radio system. Put it in the same spreadsheet as resilient vehicle broadband, HPUE, satellite, gateways, broadband PTT, targeted in-building coverage, or some combination, then ask which solution actually solves the operational problem for the money. Some of those comparisons will still produce a tower, and that is a legitimate outcome. Every tower should have to prove it is the best way to solve the requirement.

The most interesting case is an agency approaching a major LMR replacement. Before writing an RFP for \$20 million, \$40 million, or more, pull the requirements apart and ask what actually has to

be RF. An RFP written around the architecture the agency already owns should not surprise anyone when the answer comes back as a newer version of the architecture the agency already owns.

Immediate tactical voice, direct and simplex operation, IDLH and fireground communications, coverage independent of commercial networks, and emergency signaling belong on RF. LMR is very good at those. Wide-area interoperability, remote dispatch, AVL, video, routine status, messaging, out-of-area communications, and much of mutual aid probably do not. Separate those requirements and the answer may be a smaller, more focused RF investment paired with a larger investment in shared IP infrastructure. That could mean fewer towers in some places, though fewer towers is a byproduct rather than the goal.

The analog question may be even more interesting. An agency running a functional analog system should not automatically assume its next step is expensive digital trunked LMR, with broadband arriving someday after that. For some agencies the smarter move is keeping relatively simple RF for local tactical voice while putting modernization dollars into IP backhaul, broadband PTT, gateways, resilient multi-carrier connectivity, satellite, modern dispatch, identity, security, and network-level interoperability. The point is to challenge the assumption that the historical upgrade path is automatically the correct upgrade path. Ask what problem the digital radio investment is solving and whether RF is the best layer to solve it.

The financial comparison cannot reduce to a tower costing X and broadband costing Y. It has to become a question of how many operational capabilities the dollar buys, how resilient they are, and how much future flexibility the investment creates.

A workable funding philosophy looks like this. Keep mission-critical LMR healthy. Stop automatically expanding the legacy architecture without comparing alternatives. Redirect modernization dollars toward infrastructure that can support multiple applications. Use normal lifecycle replacement as the primary migration engine. Build new dedicated infrastructure when the operational requirement proves it is the best answer.

Some new money will be required at the beginning for pilots, interfaces, and gateways. Long term, the business case is not finding another \$2 million for broadband. It is changing where the existing communications capital plan puts its next \$2 million.

That is a principle rather than a plan. Appendix B turns it into one, with a phased program, rough-order-of-magnitude figures, and a first step an agency can take for under \$5,000.

A BETTER BUDGET QUESTION

Stop asking what the radio system needs next. Ask what communications capability the public safety system needs next, and which layer is the best place to buy it. That change in wording can change an entire capital plan.

SECTION 8

Standards and Vendor Independence

Broadband First cannot mean replacing one closed ecosystem with another.

If the goal is a network-centric architecture, then standards, interoperability, and vendor independence have to be part of the design from the beginning. The network should be the common layer. Applications, radios, gateways, carriers, consoles, broadband PTT platforms, and satellite providers should connect to that layer through documented and supportable interfaces wherever practical.

Every product does not have to be interchangeable. An agency should be extremely cautious, though, about designing an architecture where changing one component requires replacing everything around it. Public safety has already lived through that model. Agencies spend decades building around a single radio ecosystem because subscriber radios, consoles, infrastructure, encryption, interfaces, maintenance tools, and operational practices all become dependent on one another. Broadband is an opportunity to do something different.

This paper names specific products in the sections describing the August test, because a field demonstration runs on real equipment and readers deserve to know what was tested. Those references should be read as one implementation of the architecture rather than as the architecture itself. Every function described here, the bonded gateway, the broadband PTT platform, the radio gateway, the managed integration, and the satellite path, has more than one supplier.

Standards are an exit strategy

Standards get discussed as an interoperability feature. They are also an ownership strategy, because a standards-based interface gives an agency choices later.

If a broadband PTT platform stops meeting the agency's needs, can another application use the same network and interface with the same systems? If a cellular provider underperforms in part of the service area, can another carrier be added without redesigning the communications system? If a gateway manufacturer changes direction, can another vendor provide the same operational function? If a dispatch platform changes, can the agency preserve its radio, broadband, logging, identity, and interoperability investments?

Those questions should be answered before procurement rather than after the contract is signed.

Avoid building the next silo

A network-centric architecture can still become a silo. An agency could replace an LMR-centric environment with a broadband PTT platform that only works with one manufacturer's devices, build vehicle connectivity around a single carrier, deploy gateways that interface with one radio ecosystem, and move operational identity into a proprietary platform that cannot be exported or shared. Technically the agency would have modernized. Architecturally very little would have changed.

The objective is to make individual components replaceable without requiring the agency to replace the system.

Buy interfaces, not just features

Public safety procurement tends to focus on what a product can do. It should also ask what the product can connect to. A procurement should identify the interfaces, standards, APIs, data formats, authentication methods, logging requirements, and interoperability capabilities the agency expects. Appendix B closes with a checklist of the questions worth putting in writing before a contract is signed.

The answer does not always have to be completely open. There are legitimate reasons for proprietary technology, particularly where a manufacturer provides a highly specialized capability. What matters is that the agency knows where the proprietary boundaries sit and accepts them deliberately. Vendor dependence should be a documented architectural decision rather than something discovered five years later.

Multi-vendor should be normal

A resilient architecture should assume more than one vendor will be involved. One company may provide the radio system, another broadband PTT, another vehicle connectivity, several the terrestrial carrier service, another satellite, and another the dispatch applications. Designed

intentionally, that is a strength. No single manufacturer will always have the best radio, the best network, the best gateway, the best application, the best satellite service, and the best public safety workflow.

The August test is itself an example. Several distinct suppliers contributed components, none of them owned the whole path, and audio still crossed from a portable radio through a mobile gateway, over three carriers and a satellite constellation, into a broadband PTT platform, and out to four trunked radio systems in three states.

It is worth restating what that implies, because the debate is often framed as a binary choice. The question is not whether an agency runs LMR push-to-talk or broadband push-to-talk. Well-designed agencies will run both, and the architecture should assume it.

Vendor independence is not vendor hostility. Public safety needs strong vendor partners, because these systems are complex, operationally critical, and require companies willing to support them for years. Independence means maintaining enough architectural control that the agency remains the owner of its communications strategy. A good vendor should compete because its product performs well, integrates well, and provides value. It should not retain the customer because leaving has been engineered to be prohibitively difficult.

Test portability before you need it

If an agency claims a system is standards-based, connect something from another vendor. If a gateway is supposed to support multiple radio platforms, prove it. If operational data is supposed to be exportable, export it. If another broadband carrier is supposed to provide an alternate path, move traffic onto it. If a replacement application is supposed to work through the existing network, test the interface.

Interoperability documentation is useful. Operational evidence is better. The worst time to discover that a supposedly open interface is actually proprietary is during an emergency or immediately before a major procurement.

The long-term goal is simple. The agency should own the architecture, and vendors should provide components within it. That changes the procurement relationship. Instead of asking a manufacturer to design the agency's communications environment around its product line, the agency defines the architecture, the standards, the interfaces, the operational requirements, and the failure conditions. Vendors then compete to provide the components that best meet them.

SECTION 9

Interoperability Beyond the LMR Footprint, and What Leaders Should Do Now

The operational case for network-centric communications gets strongest when the incident stops respecting jurisdictional boundaries. Wildfire, search and rescue, severe weather, major investigations, special events, mutual aid, and disaster response routinely assemble personnel who share no radio system, no frequency band, no vendor, and sometimes no state.

LMR interoperability can be engineered for those events. It usually depends on preparation: compatible channels, programmed radios, system keys, patches, caches, talkgroup permissions, gateways, or a formal network interface. Broadband PTT gives leaders another option, because the common denominator becomes an application and an IP connection.

A Grant County responder deploying hundreds of miles away should not lose every local communications relationship by leaving the home system footprint. A dispatcher should not be tied to one building because the console historically lived there. A mutual-aid partner should not have to join the home agency's entire radio ecosystem to speak on one operational channel.

The same architecture enables remote operations

MACC already dispatches remotely, including personnel working far outside Grant County. That usually gets discussed as a staffing tool. Architecturally it is the same story as broadband radio, because the service has been decoupled from the physical location. Phones, CAD, radio, logging, connectivity, identity, and security can be assembled as network services.

Continuity of operations follows directly. If the center becomes inaccessible, a dispatcher moves. If local staffing falls short, the work moves. If one network path fails, another carries the applications.

Define success at the responder level

The final measure of a communications system is not whether the network diagram works. It is whether the responder does.

A network engineer may define success by whether an ISSI connection is established, a gateway is online, packets are flowing, encryption is functioning, or a carrier failover occurred correctly.

Those things matter. The first responder does not care how many network paths exist behind the radio. They care that they press the button and talk. A deputy in a dangerous altercation with an suspect does not care which carrier the vehicle gateway selected. They care that the emergency button works. A medic does not care which cloud service delivered the premise information. They care that it was available before walking through the door. A dispatcher does not care whether audio arrived through RF, cellular, satellite, or microwave. They care that they heard the unit, knew who was talking, knew where they were, and could respond immediately.

That should be the acceptance test.

A communications workflow that works while standing next to a technician during a demonstration may not work during an emergency. Responders use these systems while driving, wearing gloves, treating patients, operating apparatus, searching buildings, managing rapidly changing incidents, and physically dealing with offenders. The system should be designed and tested under those conditions.

A responder-level acceptance test should ask:

- How many steps are required to establish the communications path?
- Can the user accomplish the task without understanding the underlying architecture?
- Can it be done while wearing PPE or operating another piece of equipment?
- Does the emergency button behave predictably?
- Does unit identification survive across the communications path?
- Does dispatch know who is talking and where they are?
- Does the system continue operating when a carrier or network path fails?
- Is there an obvious and familiar degraded mode when something does fail?
- Can a user who was not part of the project team operate it successfully?
- Do responders trust the system enough to use it during an actual emergency?

That last question may be the most important, because usage is evidence. If an agency builds an interoperability capability and responders consistently avoid it, the first conclusion should not be that more training is required. The agency should ask whether it engineered the right solution.

Predictability is what builds the trust. Common channels and talkgroups should appear in predictable locations. Naming should stay consistent across devices and agencies where practical. Gateway functions should behave consistently. Emergency signaling should not change unexpectedly because traffic crossed from one network into another. Consistency reduces cognitive load, predictability creates confidence, and confidence creates use.

Public safety technology projects often measure completion through technical milestones. A gateway was installed. A radio was programmed. An interface went live. A broadband network reached a coverage target. Those are implementation measures rather than measures of operational success. The better question is whether the responder received the right communications capability and the right information, at the right time, with the least reasonable effort. The best network in the world has very little value if the person at the end of it cannot, will not, or does not know how to use it when the emergency occurs.

What leaders can do this year

- Run Year Zero. Under \$5,000, no procurement cycle, and a first-hand opinion within a month.
- Inventory workflows, not just equipment. Identify what information moves today, which medium carries it, and whether that medium actually fits.
- Measure your radio traffic. Find which routine transmissions can migrate to CAD, AVL, secure messaging, or automation.
- Test the ugly details. Emergency button behavior, encryption, unit identification, recording, console presentation, gateway transmit restrictions, dead zones, device management, cybersecurity, and failure modes matter more than a clean vendor demonstration.
- Rewrite procurement language. Specify outcomes, standards, interfaces, failure-domain diversity, portability, and lifecycle cost.
- Plan for the people side. Governance, training, operating procedures, security, fleet management, and user confidence have to mature alongside the architecture.

Interoperability that exists only in a diagram is not interoperability. The system becomes real when dispatchers and responders know how it behaves under stress and use it often enough that it is not a science project on the day of the emergency.

SECTION 10

Conclusion

The August 2026 test began as an interoperability exercise and ended by raising an architectural question. Those results do not make traditional radio obsolete. They make an LMR-only investment framework obsolete.

What follows from that is a timing problem more than a technology problem.

Most agencies reading this will face a radio system decision within five years. Some are drafting the RFP now. The architecture gets fixed at the moment the specification is written, well before the system goes live, and it stays fixed for the twenty years that follow. An agency that writes its next specification around the system it already owns will get a newer version of that system, then discover afterward that the capabilities it wanted have to be purchased separately, on top, at additional cost.

That is the practical risk of drifting. The danger is not that a legacy system fails. The danger is that an agency buys the same capability twice and pays more for the version that does less.

The future is broadband as the primary communications platform, with LMR retained where RF remains the best tool. Maintain LMR where it is strong. Use broadband to extend it, connect it, reduce unnecessary traffic on it, and carry the information LMR was never designed to handle. Shift new investment toward the layer that creates the most capability and the most resilience.

None of that requires a bond measure to begin. It requires one radio, one interface, and a week of somebody's attention.

The battalion chief asked the right question, and increasingly the answer is that we can. The remaining work is writing the governance, standards, operating model, and procurement language that let public safety use what is already here, and doing that work before the bond measure goes to the voters.

APPENDIX A

The Field Test in Detail

This appendix documents the August 5 and 6, 2026 field test at MACC911 in Moses Lake, Washington. It names specific products because a demonstration runs on real equipment and a reader evaluating this architecture needs to know what was actually in the room.

The failures are reported alongside the successes, in the same level of detail, because that is the part most useful to an agency planning its own test.

A.1 Purpose and design

The test set out to answer three practical questions.

- How quickly can agencies running different, unconnected radio systems be brought onto a common talkgroup?
- How does a blended broadband architecture behave when individual network paths are removed while traffic is live?
- How useful does a portable radio remain when a public safety vehicle becomes the bridge between LMR RF and broadband?

Scenarios were ordered by increasing difficulty, starting from a known RF baseline and progressing to environments where conventional coverage fails. The written plan stated that not everything had to work and that field failures were useful. That framing mattered, because several things did fail.

A.2 Participants

More than sixty public safety professionals attended, drawn from fire, law enforcement, corrections, emergency management, and communications centers.

- Host and co-hosts were MACC911, with D.T. Donaldson and Gerrit Klein running the operational side. Brent VanKeulen facilitated.

- Vendor participants on site were EF Johnson Technologies, with Rudy Torres; ESChat, with Shawn Moreno; Dejero, represented by Michael Stanton; IP Access International, represented by Bryan Hill; and Silvus Technologies for the MANET segment.
- Remote participants included the New Mexico State Police and LA County RICS. New Mexico monitored the full session and recorded the day's traffic.

A.3 The architecture under test

The signal path being tested ran as follows.

Portable radio in direct mode, to vehicle-mounted VM8000 in gateway mode, to Dejero GateWay blended broadband, to ESChat core, out to dispatch console, other LMR systems, and broadband devices.

Each element played a specific role. The portable operated conventionally, on a simplex channel, with no dependency on a repeater or tower. The VM8000 mobile radio received that direct traffic and bridged it onto IP. The Dejero device aggregated multiple broadband paths into a single managed connection out of the vehicle. ESChat carried the voice as broadband push-to-talk and connected outward to P25 systems through ISSI and to other LMR systems through gateway interfaces.

The lead vehicle carried five simultaneous connections: Starlink, FirstNet with HPUE, AT&T, Verizon, and T-Mobile.

A.4 Configuration

ELEMENT	CONFIGURATION
Interop Alpha	Channel 03, broadband and LMR
Interop Bravo	Channel 04, broadband only, no LMR infrastructure
D1	Direct and simplex channel used by portables reaching a vehicle gateway
Gateway activation	Long press on a soft menu button, chosen deliberately to prevent accidental activation
Gateway output	Interop Alpha

ELEMENT	CONFIGURATION
Gateway path behavior	Outbound simplex traffic routes over broadband only. Inbound accepts both LMR and broadband
Local network	Dedicated SSID for the exercise, with a Dejero Titan go-kit providing connectivity inside the meeting venue
Vehicles	Three rigs configured in gateway mode, soft-installed the evening before

Two fire rigs were still being soft-installed the night before the test. Programming templates were prebuilt, so configuration was fast, while physical mounting and cabling took the time. Direct mode had not been confirmed working on the mobile radios as of the evening of August 5, and was completed before the morning session.

A.5 Morning session: Moses Lake City Council Chambers

Tests ran in front of the full audience, starting from a known reference point.

TEST	RESULT
VP8000 to VP8000, direct mode, no infrastructure	Pass. Established the audio quality and delay baseline against which everything else was judged
Portable through the trunked repeater	Pass. Second reference point
ESChat on an Android handset receiving trunk traffic over cellular	Pass
VP8000 with antenna physically removed, Wi-Fi only, to MACC911 dispatch via ESChat	Pass
Live failover, antenna pulled mid-transmission	Pass. Switched to Wi-Fi in roughly three to four seconds with no audible drop
Blended baseline across five paths	Pass
Carrier removal, one at a time: Verizon, then FirstNet AT&T, then T-Mobile	Pass. No loss of signal and no perceptible transmission delay at any stage

TEST	RESULT
Satellite-only fallback	Pass. Starlink carried the final leg. Observers watching the Dejero dashboard could see traffic redistributing across paths in real time
Gateway mode to LA County RICS: VM8000 on Interop Alpha, Tait portable on D1	Pass. Traffic reached LA County RICS in real time from roughly six hundred miles away
Broadband push to talk group on Interop Bravo	Pass. Voice communications operated over broadband without LMR infrastructure in the wide area path.
Multiple radio manufacturers through the VM8000 gateway	Pass. Tait and Kenwood portables and an Android handset passed traffic to the same talkgroup.

The interoperability demonstration was the centerpiece. Four trunked systems operated on a common talkgroup: MACC911, LA County RICS, the New Mexico State Police, and Spokane. LA County, San Luis Obispo, and MACC911 were already linked through ISSI on the ESChat server. Spokane and New Mexico had no prior connection to MACC and were each brought in during the exercise, over the phone, in roughly ten to fifteen minutes.

One moment during the session illustrated the bring your own radio argument better than the equipment did. A Grant County deputy, working through the channel plan, found an 800 MHz mutual-aid channel already programmed in his radio that he had not known was there.

A.6 Midday: Moses Lake Police Department and basement

The group moved across the street to test in-building performance in a structure with poor RF and no usable cellular signal below grade.

Three vehicles were placed in gateway mode simultaneously. Two testers took portables set to D1 into the basement, following a first-arriving-unit sequence: press the gateway button on the mobile, switch the portable to the direct channel, then leave the vehicle and work normally.

One tester reached the furthest accessible point in the basement, with no cellular signal available. Voice traffic still moved from the basement, to the vehicle, onto broadband, and into the trunked system.

The multi-gateway result was the surprise of the day. All three rigs received and repeated the same transmission. The system self-selected a single gateway to pass the traffic, with no collision,

no duplicate audio, and no feedback. The tester in the basement was unaware that three gateways were running. The working explanation is that the trunked system denied simultaneous transmissions and admitted one, with the first gateway to win the contest carrying the traffic. That result is what prompted the open architectural question in Section 4.

Two problems surfaced here. One radio was unexpectedly transmitting and had to be limited to a single band. Something in the area disrupted phone connectivity and interfered with ESChat, and the team fell back to a cell call to complete the final sound check.

A.7 Afternoon: jail and wildland

At the jail, a deputy chief carried a portable into a known dead zone and stayed connected through the vehicle gateway. His summary of the result, delivered on the spot, was that he had just walked into the dead zone and gotten out.

The wildland and driving scenario tested range from a portable in direct mode to a vehicle acting as the only infrastructure. Push-to-talk held at approximately 4.7 miles. This segment drew the strongest reaction from field personnel.

A.8 MANET

Silvus Technologies provided ground-based mesh nodes.

The assessment was mixed and worth stating plainly. The mesh performed, and setup complexity was high enough that the team did not consider it suitable for ad hoc configuration at an incident. The complexity sits in the wrong place. Dynamic mesh topologies of the kind proposed for Sidelink, where devices opportunistically provide connectivity to one another as needed, become far more useful when the mesh capability is native to the handset and requires no user interaction at all. It needs pre-engineered deployment. A compact satellite terminal now fills much of the same operational gap at a fraction of the cost and effort, which changes the calculation for most agencies most of the time.

A.9 What did not work

ISSUE	DETAIL AND STATUS
Intermittent ISSI dropout	Audio reached ESChat handsets reliably but did not always make it back out to the dispatch trunk. Suspected causes are ISSI misconfiguration, gateway console settings, or site affiliation bounce. The talkgroup was configured quickly on the day without full research, so configuration is the leading explanation. Not yet reproduced under controlled conditions. Action item is a bench test with a controlled mobile gateway and portable under signal stress
Emergency button behavior	The emergency alarm data packet does not pass through the gateway. The emergency call does. On the systems tested, the alarm passed only on Motorola. P25 emergency button activation also lets a system administrator choose whether the emergency reverts to a dedicated emergency talkgroup or broadcasts on the channel the radio is resting on, so knowing how each participating system is configured matters before designing around it. Workaround is to press the emergency button and then transmit. This needs documenting device by device and system by system before any agency writes an operational protocol around it
Mobile transmit disabled in gateway mode	A crew cannot talk on the mobile radio while that radio is serving as the gateway. A fire chief flagged this immediately. The practical workaround is a portable, which most vehicles already carry. Whether transmit can be enabled on the mobile in gateway mode is an open product question
Unit identification	The dispatch display shows the gateway radio ID rather than the originating portable ID. Agencies can work around this by identifying which gateway is transmitting. Portable ID pass-through is pending a software update

ISSUE	DETAIL AND STATUS
Wi-Fi-only mobile transmissions not heard at dispatch	Observed once during the morning session. Root cause and operational significance were not established.
Poor audio during the council chambers segment	The team attributed the poor audio to the building structure and low microphone input. This explanation was observational and was not confirmed through controlled testing.
Garbled encrypted audio	Traced to a missing Wi-Fi antenna on a mobile radio. Without it the broadband connection was too weak to carry encrypted audio end to end. The first part of each transmission was clear and garbling began on the return path through the gateway
Radios not preprogrammed for direct mode	Several portables required manual channel changes during the exercise. Nothing failed as a result. It cost time an emergency would not have provided
Spokane missed traffic	No second radio was available at the Spokane end, so the gateway there could not participate fully. A logistics gap rather than a technical one

A.10 Security, raised from the floor

An emergency manager in the audience raised internet-based communications as a cybersecurity risk. The question was not planted and it deserves the direct answer it received.

The bonded broadband transport used in the test operates at FedRAMP Moderate. The broadband PTT platform holds FedRAMP authorization. Modern smartphones support strong device and transport encryption. LMR traffic during the test was intentionally left unencrypted for convenience, and would be encrypted in any operational deployment.

The broader point belongs in every evaluation of this architecture. Security has to be assessed layer by layer, at transport, application, device, and RF, rather than as a single question about whether the internet is safe. Cybersecurity is more effective when it is baked in than when it is bolted on, which is an argument for addressing it in Year One of any migration rather than after the architecture is in service.

A.11 What we would do differently

- Program every portable for the direct channel before the day, and verify it. Manual channel changes during a live demonstration are a preventable cost.
- Confirm gateway configuration on every mobile radio a full day earlier. Direct mode was still unconfirmed the evening before.
- Send a second radio to every remote gateway site. Spokane could not participate fully for want of one.
- Reserve controlled bench time before the public day to characterize ISSI behavior, rather than configuring a talkgroup the morning of and discovering its edge cases in front of sixty people.

APPENDIX B

A Practical Migration and Investment Plan

Section 7 argues that the next communications dollar should go to the layer creating the most capability and resilience. This appendix is the practical version of that argument: what a phased program looks like, roughly what it costs, and where an agency starts.

A Broadband First strategy does not mean replacing the radio system tomorrow, abandoning infrastructure that works, or betting the agency on one carrier, one vendor, or one new technology.

The practical approach is simpler. Keep the existing LMR system in service. Start building a resilient broadband layer alongside it. Move capabilities to that layer when there is a clear operational reason. Measure the results. If it works, expand it. If it does not, fix it before spending the next dollar.

The figures below are rough-order-of-magnitude planning numbers. They are not vendor quotes and should be treated with a variance of at least 30 to 40 percent. They exist to show scale and give agencies something to compare against a capital plan. For discussion purposes, assume a regional agency with an existing LMR system and roughly sixty first-out or operationally significant vehicles.

B.1 Year Zero: connect one radio to broadband

BUDGETARY ROM: UNDER \$5,000

Before any of what follows, an agency can test the central claim of this paper for the cost of a single mobile radio.

The components are deliberately unglamorous. An existing LMR radio, a low cost gateway, and a commercially available push-to-talk application are enough to prove both halves of the concept: that LMR and broadband can be bridged, and that broadband push-to-talk has standalone value where it applies. For a small agency or one on a tight budget, that combination turns an abstract architectural argument into something the chief can hold in their hand.

Take one mobile or portable radio the agency already owns. Add a gateway interface, a broadband PTT subscription for a small handful of users, and a commercial data connection, which in most cases is an existing smartphone or vehicle router. Put one talkgroup on the network. Then let a dispatcher and two field users work with it for a week.

Confirm that audio moves in both directions. Check how the emergency button behaves when traffic crosses between systems. Notice what unit identification looks like on the dispatch side. Find out whether the audio quality is acceptable to the people who would have to rely on it.

The value here is not the technology. It is that a chief, a director, or a technical services manager can authorize this without a board vote, a bond measure, or a procurement cycle, and can form a first-hand opinion within a month. Nothing else in this migration path should be funded before someone inside the agency has done this and decided for themselves whether the architecture is real.

Most agencies discover two things. The core function works better than expected, and the operational details around it need more attention than expected. Both findings are worth having before Year One.

B.2 Year One: connect what we already have

BUDGETARY ROM: \$200,000 TO \$300,000

Year One is about proving the architecture without changing how responders do their jobs. The radio system stays exactly where it is. Dispatchers continue dispatching. Responders continue carrying their radios. The investment creates a reliable IP path around and beyond the existing RF footprint.

- Establish an IP path for selected radio traffic using ISSI, gateways, or other appropriate interfaces.
- Deploy broadband PTT in a controlled environment.
- Equip approximately eight to ten command or first-out vehicles with resilient broadband, using more than one genuinely diverse network path.
- Begin cybersecurity, identity, device-management, logging, and access-control work immediately.
- Train a small group of dispatchers, responders, supervisors, and technical staff.
- Document what works, what fails, and what behaves differently than expected.

The goal at the end of Year One is not agency-wide deployment. The goal is proving that voice can move between LMR and broadband users, that the network survives individual path failures, and that the agency understands the architecture well enough to decide whether it deserves another year of investment.

Year Two should not be automatic. The architecture should have to earn it.

B.3 Year Two: extend the edge

BUDGETARY ROM: \$275,000 TO \$375,000

If Year One works, Year Two moves resilient connectivity closer to the responder. Roughly twenty additional first-out law enforcement, fire, EMS, command, or specialty vehicles get equipped with resilient broadband and, where appropriate, radio gateway capability. That may include multiple cellular carriers, FirstNet and HPUE where they provide an operational advantage, satellite where geography or mission justifies it, vehicle Wi-Fi, broadband PTT, local radio gateways, and coverage monitoring.

Not every vehicle needs every capability. A command vehicle operating in remote wildland areas may justify multiple carriers and satellite service. An administrative vehicle operating inside good commercial coverage probably does not. Design around operational risk instead of equipment uniformity.

Year Two is also when the agency should intentionally start breaking things. Take away a carrier. Block satellite. Shut down a gateway. Lose a backhaul path. Drive outside normal coverage. Find out what continues to work. It is much better to learn that on a Tuesday afternoon than during a wildfire.

B.4 Year Three: move information off voice

BUDGETARY ROM: \$425,000 TO \$550,000

By Year Three the network should be mature enough that broadband is no longer viewed primarily as a backup. This is where the agency substantially completes the vehicle deployment, potentially reaching roughly sixty operational vehicles, and shifts focus from connectivity itself to what moves across it.

Routine radio traffic should be reviewed honestly. Status changes, location checks, records returns, routine dispatch details, premise information, images, and administrative coordination may be better handled through CAD, AVL, secure messaging, or automation. Officer emergencies, pursuits, maydays, IDLH fireground operations, and rapidly changing tactical events remain immediate shared voice. The goal is not reducing radio traffic because radio traffic is bad. The goal is using each medium for what it does best.

B.5 Year Four: integrate operations

BUDGETARY ROM: \$225,000 TO \$425,000

By Year Four the technology should stop feeling experimental. Broadband PTT, gateways, LMR, dispatch, mobile devices, remote operations, and interoperability should function as parts of one communications environment.

A mutual-aid responder should not need to be programmed into the host radio system, carry one of its radios, or understand its entire communications architecture just to participate on one operational channel. Depending on the incident, that user may enter through broadband PTT, an ISSI connection, a gateway, another LMR system, or another network path. The common point is no longer the radio system. It is the network.

Year Four should also bring much more mature governance. Who creates users? Who approves access? Who manages gateways? Who owns recording? How are incident channels created? What happens when a user leaves an agency? How are devices secured? What information is retained? How is encryption and identity managed across organizations? Technical interoperability without administrative interoperability is not really interoperability.

Procurement should begin changing here too. RFPs should describe the result the agency needs, the interfaces it requires, the failure conditions the system must survive, and the standards vendors must support. An RFP written around the architecture the agency already owns should not surprise anyone when the answer is a newer version of the architecture the agency already owns.

B.6 Year Five: change the capital plan

BUDGETARY ROM: \$175,000 TO \$350,000

By Year Five the agency should have enough operational experience and real data to stop treating the radio system as its own investment category. The question stops being what the radio system needs next. It becomes what communications capability the agency needs next, and where is the best place to buy it.

Sometimes the answer will still be a radio tower. Fixed, engineered RF coverage does not depend on a vehicle being nearby, can be designed to a known coverage standard, and can be hardened for a specific service area. That has real value. The tower should have to compete for it. Could the problem be solved with vehicle gateways, additional broadband coverage, satellite, an in-building solution, a deployable node, a different backhaul path, or several smaller solutions combined? Those options belong in the same spreadsheet.

B.7 What the program costs

YEAR	APPROXIMATE INVESTMENT
Year Zero	Under \$5,000
Year One	\$200K to \$300K
Year Two	\$275K to \$375K
Year Three	\$425K to \$550K
Year Four	\$225K to \$425K
Year Five	\$175K to \$350K
Five-year total	Approximately \$1.3M to \$2.0M

These are planning numbers, not bids.

The largest early capital expense is the vehicle edge. MACC911's planning experience puts a well-equipped resilient broadband vehicle package at roughly \$10,000 per vehicle depending on configuration. At that level, sixty vehicles represents roughly \$600,000 in equipment and deployment before recurring network services. The remainder of the program is what makes the equipment useful: interoperability, broadband PTT, applications, cybersecurity, integration, testing, training, governance, and lifecycle management.

Recurring costs also increase as the architecture matures. Carrier service, satellite connectivity, software licensing, support, device management, cybersecurity, and replacement cycles do not disappear because the equipment is distributed. A mature deployment could reasonably create additional recurring communications expense in the range of \$150,000 to \$200,000 annually depending on how aggressively cellular, satellite, and broadband PTT services are deployed. That number needs to be evaluated against what it buys, and against the lifecycle cost of the infrastructure the agency already owns.

A five-year program costing \$1.3 million to \$2 million is not inexpensive. Neither is maintaining a mature radio system. The correct question is which investment gives responders and dispatchers the most capability, resilience, and flexibility for the next dollar spent.

B.8 Each phase should earn the next one

One difference between this approach and a traditional system replacement matters more than any of the numbers. The agency does not have to commit to the entire program on day one.

Spend under \$5,000 in Year Zero. Build the foundation in Year One for \$200,000 to \$300,000. Use it. Test it. Break it. Measure it. Ask the responders and dispatchers whether it actually made their jobs better. Then decide whether Year Two deserves funding, and apply the same standard every year after.

Broadband First should not become another technology assumption that receives money because the organization started down that road. It should have to earn the next dollar too. That is the point.

B.9 Lifecycle replacement as the migration engine

For agencies without a large capital project on the horizon, the transition can happen quietly through normal replacement cycles.

- Router dies. Replace it with resilient multi-path connectivity.
- Command vehicle gets replaced. Build the connectivity architecture into it.
- Gateway reaches end of life. Replace it with something IP-capable and interoperable.
- Microwave gets refreshed. Treat it as resilient general-purpose transport instead of radio backhaul alone.
- New console project. Require standards-based interfaces and remote IP capability.
- CAD replacement. Require it to operate independent of one physical dispatch center.

In that model Broadband First stops being another massive capital project sitting beside the radio budget. The lifecycle replacement process becomes the migration strategy.

B.10 A procurement checklist

Section 8 argues that an agency should buy interfaces rather than features alone. These are the questions worth answering before a contract is signed, not after.

- Does the product support recognized industry standards where those standards exist?
- Are APIs documented and available to the agency?
- Can another vendor integrate without requiring the original manufacturer to build a custom interface?
- Can identity and permissions be managed outside the product?
- Can configuration and operational data be exported?
- Can logs and recordings be retained independently?
- Can the agency change network providers without replacing the application, and change the application without replacing the network?
- Can the gateway communicate with more than one radio manufacturer or technology?
- Who owns the data the system generates, and what happens to that data and configuration when the contract ends?

APPENDIX C

Glossary

AVL (Automatic Vehicle Location). GPS-based tracking that shows dispatch where each unit is in real time.

Band 14. The dedicated block of radio spectrum reserved for FirstNet public-safety broadband.

Blended (bonded) connectivity. Combining several network connections, multiple cellular carriers plus satellite, into one managed link, so traffic uses whatever paths are healthy.

Broadband. High-capacity, internet connectivity (cellular, satellite, Wi-Fi, fiber) able to carry voice, data, video, and applications on one network.

CAD (Computer-Aided Dispatch). The software dispatchers use to create and manage incidents and track units.

Console. The dispatcher's control position for monitoring and transmitting on radio systems.

Direct mode (simplex). Radios talking directly to each other, radio-to-radio, with no tower or repeater. Short range, but works when infrastructure is gone.

Encryption. Scrambling communications so only authorized parties can understand them.

Failure domain. A group of things that can fail together because they share something, such as the same conduit, power source, or provider. True resilience requires paths that do not share failure domains.

FedRAMP. A U.S. government program that certifies the security of cloud services. "Moderate" is one of its impact levels.

FirstNet. The nationwide public-safety broadband network (on Band 14) that gives first responders priority and preemption over commercial users.

Gateway. A device that bridges radio (RF) traffic onto the broadband and IP network and back, letting radios reach systems far beyond their normal coverage.

HPUE (High-Power User Equipment). Cellular devices that transmit at higher power, up to about six times normal, on FirstNet's Band 14, improving range and in-building coverage.

IDLH (Immediately Dangerous to Life or Health). Conditions such as interior firefighting where reliable, immediate communication is critical.

Interoperability. The ability of different agencies and systems to communicate with one another.

IP (Internet Protocol). The common standard for moving data across modern networks, the language that lets radios, phones, video, and applications share one network.

ISSI (Inter-RF Subsystem Interface). A P25 standard interface that formally connects two separate radio systems so their users can share talkgroups. The engineered way to link systems, versus a gateway.

Jitter. Variation in network delay. High jitter degrades voice quality.

Latency. Delay, meaning how long it takes data to travel from one end to the other.

LEO satellite (Low Earth Orbit). Satellite service, such as Starlink, that orbits close to Earth, giving lower delay than traditional satellites and an additional, independent network path.

LMR (Land Mobile Radio). Traditional two-way public-safety radio, including portables, mobiles, towers, and repeaters.

MANET / mesh (Mobile Ad Hoc Network). A network the devices form among themselves, each relaying for the others, with no fixed infrastructure.

Mission-critical push-to-talk (MCPTT). Standards-based push-to-talk voice over broadband, built to meet public-safety requirements.

NENA i3. The standard architecture for Next Generation 911 that separates services and applications from the underlying network.

NG911 (Next Generation 911). The modern, IP-based replacement for legacy analog 911 telephony.

P25 (Project 25). The North American standards for digital public-safety radio, designed so compliant radios and systems can interoperate.

Packet / packet-level routing. Data travels in small units called packets. Packet-level routing sends each packet across whichever connection is healthiest at that instant, rather than committing to one link.

Preemption. The ability to bump lower-priority commercial users off a congested network so public-safety traffic gets through.

Priority. Guaranteed preferential access to network capacity for public-safety users.

PSAP (Public Safety Answering Point). A 911 call center.

PTT (Push-to-Talk). Press-to-talk voice communication, whether over radio or broadband.

Quality of Service (QoS). Network features that prioritize important traffic so it performs reliably.

Redundancy vs. resilience. Redundancy is a spare waiting behind the primary. Resilience is the mission continuing across many paths and modes even as individual components fail. The paper argues for resilience.

Repeater. Equipment, on a tower or in a vehicle, that receives and rebroadcasts radio signals to extend range.

RF (Radio Frequency). The wireless spectrum radios use to transmit.

RFSS (RF Subsystem). A core controlling component within a P25 radio system.

ROM (Rough Order of Magnitude). A ballpark planning cost estimate, not a vendor quote.

Sidelink. A cellular standard that lets devices talk directly to each other without going through the network, the industry path toward mesh-like capability built into handsets.

SIM. The card or profile that identifies a device on a cellular carrier. Multiple SIMs let one device use multiple carriers.

Talkgroup. A virtual channel on a trunked or IP system. Everyone assigned to the same talkgroup hears each other.

Trunked radio. A system that automatically shares a pool of channels among many talkgroups using a controller, which is more efficient than fixing one channel per group.

Acknowledgments

The August 2026 field demonstration at MACC911 happened because four companies sent people and equipment to central Washington and let their technology be tested in public, in front of sixty working professionals, with no guarantee of a flattering result. Several of the findings in this paper are open items rather than successes. That the partners below were willing to have those documented alongside the wins says something about how they approach this work.

Their participation is gratefully acknowledged. It is not an endorsement of any product by the authors, and no partner reviewed or approved this paper before publication.

The authors thank the following organizations and the individuals who made the demonstration possible.

ORGANIZATION	CONTRIBUTION	CONTACT
EF Johnson Technologies a JVCKENWOOD company Irving, Texas www.efjohnson.com	VP8000 portable and VM8000 mobile radio platforms, gateway configuration and connections to Spokane and New Mexico, and field engineering support	Rudy Torres Channel Sales Director, West Region RTorres@efji.com
ESChat www.eschat.com	Broadband cybersecure push-to-talk platform, ISSI and gateway interconnection, and multi-system talkgroup configuration during the exercise.	Shawn Moreno Filed Applications Engineer shawn.moreno@eschat.com
Dejero www.dejero.com	GateWay devices and Smart Blending technology providing the blended cellular and satellite transport tested throughout the demonstration	Michael Stanton Director, Americas michael.stanton@dejero.com
IP Access International San Juan Capistrano, California www.ipinternational.net	Systems integration, managed connectivity across LEO satellite and cellular paths, field services, and support for the blended architecture.	Bryan Hill Chief Executive Officer bryan.hill@ipinternational.net

Silvus Technologies provided MANET equipment for the mesh segment.

Thanks are also due to the agencies that connected their radio systems on short notice, including LA County RICS, the New Mexico State Police, and Spokane, and to the MACC911 staff who hosted, configured, and documented two long days of testing.

Sources and Method Notes

1. MACC911, "Broadband First: A Strategic Investment Framework for Public Safety Communications," Outline v4, August 2026. Internal working document summarizing the August 5 and 6 field demonstration and observed results.
2. First Responder Network Authority, "June 3GPP meetings mark beginning of 6G era for public safety," July 29, 2026. <https://firstnet.gov/newsroom/blog/june-3gpp-meetings-mark-beginning-6g-era-public-safety>
3. First Responder Network Authority, "FirstNet Authority Emergency Management Guide" overview. <https://firstnet.gov/newsroom/blog/3-highlights-updated-firstnet-authority-emergency-management-guide>
4. Dejero, "Smart Blending Technology." <https://www.dejero.com/smart-blending-technology/> Integration and managed support of MACC's blended cellular and satellite paths provided by IP Access International. <https://www.ipinternational.net/>
5. ESChat, "Interoperability" and product overview. <https://eschat.com/interoperability/>
6. MACC911 exploratory internal analysis, 2026. AI-assisted categorization of 1,000 consecutive law enforcement radio transmissions from a randomly selected continuous period. Results should be treated as an operational sample, not a generalizable scientific estimate.
7. National Emergency Number Association, NG911 standards and i3 architecture resources. <https://www.nena.org/page/standards>
8. First Responder Network Authority, "Deployables." <https://firstnet.gov/network/TT/deployables>
9. MACC911 Technical Services Management Report, April 9, 2026; MACC Board Resolutions 02-2025 and 03-2026; vehicle and remote connectivity procurement records; related internal planning materials. Per-vehicle package figures reflect MACC planning for a configuration built on Dejero GateWay hardware and should not be read as a market price across suppliers.
10. Clackamas County, Oregon, public records regarding Measure 3-476 and the C800 public safety radio replacement project. <https://dochub.clackamas.us/documents/drupal/de2fe343-981d-4752-985e-4c8c6d8b5118>
11. EF Johnson Technologies, VP8000 portable and VM8000 mobile radio platforms. <https://www.efjohnson.com/>

Additional implementation references

- FirstNet Operations Manual overview (2026).
<https://firstnet.gov/newsroom/blog/optimizing-public-safety-broadband-firstnet-operations-manual>
 - Dejero public safety vehicle connectivity overview.
<https://www.dejero.com/blog/emergency-vehicles-at-the-center-of-critical-communications/>
 - EF Johnson Technologies. <https://www.efjohnson.com/>
 - ESChat broadband PTT overview. <https://eschat.com/>
 - IP Access International managed connectivity overview. <https://www.ipinternational.net/>
-

About the Authors

Brent VanKeulen brings 30 years of fire service experience, most notably with Tualatin Valley Fire and Rescue and the Western Fire Chiefs Association, where he remains active today. His focus is first responder safety and operations, with a career built on connecting first responders with the critical information and capabilities that drive both safety and performance in the field.

D.T. Donaldson is Director of MACC911 in Grant County, Washington, where he focuses on modernizing public safety communications and using technology to improve resilience, workforce sustainability, and service delivery. His work emphasizes systems thinking and challenging legacy assumptions about how public safety services must be delivered.

Gerrit A. Klein is Technical Services Manager at MACC911 in Grant County, Washington, where he leads technology, communications, and infrastructure initiatives supporting 911 operations. With more than two decades of public safety experience spanning dispatch, law enforcement, fire/EMS, and technical services, his work focuses on building resilient systems, advancing interoperability, and using emerging technology to improve how first responders and 911 professionals operate in the field.