A Corrective Framework for Vermont Public Safety Communications

Resilience • Redundancy • Governance • Accountability

Prepared for Legislative and Policy Review

Including:
• Predictable Failure Scenarios
• Documented Warnings and Foreseeability
• Governance and Oversight Gaps
• Implementation Pathways

February 22, 2026
Version: 1.5

by Irene Wrenner, et.al.

TABLE OF CONTENTS

Executive Summary

Corrective Strategy for Vermont Public Safety Communications, Dispatch, and Telecommunications Infrastructure

Purpose and urgency

This corrective report is submitted in response to the Public Safety Communications Task Force's final report and the State's continued movement toward major technology procurements *without* the foundational planning required by law, engineering practice, or public accountability.

The risk is not abstract. Vermont is at a point where decisions made in the next year—particularly regarding dispatch systems, radio infrastructure, and statewide data platforms—will either correct a decade of structural failures or lock them in at vastly greater cost.

This report is not a protest. It is a course correction: a fact-based explanation of what has not been completed, why that matters, and how Vermont can still recover value, public safety, and trust.

What the Task Force report acknowledges—and does not

The Task Force report is significant in one respect: it publicly acknowledges, for the first time, the failure of the Lifeline/VCOMM system. Tens of millions of dollars—primarily from federal Homeland Security grants—were spent on a statewide radio system that was grossly underutilized, never met its intended coverage or reliability goals, and has now been dismantled.

That acknowledgment matters. But it is not enough.

The report then proposes new statewide technology investments—particularly a statewide computer-aided dispatch (CAD) system and a statewide VHF radio simulcast concept—without completing the statutory prerequisites, engineering analyses, governance structures, or revenue models required to sustain those investments.

This repeats the same pattern that produced Lifeline/VCOMM.

Statutory requirements that remain unmet

Act 78 (2023 Appropriations Bill sec. C.114)

Act 78 – see Appendix E – did not authorize implementation. It authorized **planning**. Among its explicit requirements were:

- A complete inventory of existing dispatch, radio, and communications infrastructure
- Propagation and coverage analysis for land mobile radio (LMR) and broadband (LTE)
- Analysis of current dispatch expenditures statewide
- Forecasting of lifecycle costs and sustainable revenue sources
- Resolution of access to critical data sets necessary to perform this work

These deliverables were required before major spending decisions.

They were not completed.

Act 87 (2024 Budget Adjustment Act)

Act 87 – see Appendix E – attempted to correct the course. It unified oversight of:

- Approximately $11 million in State general funds originally appropriated for regional dispatch planning, and
- $9 million in congressionally directed spending routed through the Department of Public Safety.

Act 87 did **not** eliminate funds. It imposed conditions, timelines, and coordinated review precisely because earlier spending occurred without adequate planning.

Despite this corrective intent, the Task Force report does not meaningfully address how Act 87 altered responsibilities, constraints, or sequencing. As a result, the report's recommendations float free of the statute intended to discipline them.

Act 87 required an ongoing, bidirectional information flow with the Public Safety Communications Task Force, as federal requirements evolved and as spending plans were revised.

Based on review of available Task Force minutes and meeting transcripts, and informal inquiry to Task Force members, it is unclear whether updated information for the congressionally directed funds was shared with the Task Force after initial discussions.

If information was not shared, Task Force deliberations and recommendations would have proceeded without the full context required by Act 87.

Such uncertainty underscores the need for explicit, auditable reporting checkpoints and shared visibility into funding status and sequencing, as proposed in this report.

Independent expert review (3 V.S.A. § 3303)

For more than 30 years, Vermont law has required an independent expert review before major state technology investments, including:

- Architecture review
- Lifecycle cost analysis
- Risk assessment

Such an independent review was not done before substantial portions of the congressionally directed $9 million was spent. It was not complied with for Lifeline/VCOMM. The Task Force report does not acknowledge this failure.

Proceeding again without such a review would repeat a known violation of law.

Telecommunications planning failure as a root cause

These failures do not stand alone. They are inseparable from Vermont's broader telecommunications planning failure.

During the public comment process for Vermont's **Ten-Year Telecommunications Plan adopted June 30, 2021**, detailed testimony was submitted urging:

- Hardened and resilient fiber routing
- Backup power requirements
- Integration of public safety needs into infrastructure planning

As documented in **Appendix G** of that plan, the Department of Public Service repeatedly dismissed these concerns as "outside the scope" of the plan.

The consequence is not theoretical. Vermont proceeded to spend hundreds of millions of dollars on broadband deployment without creating:

- Open-access resilient fiber rings,
- Hardened backhaul suitable for public safety radio and LTE infill, or
- Enforceable backup power standards for emergency communications.

Four representative excerpts are highlighted in this executive summary to make clear that these issues were raised, documented, and rejected.

Vermont is now living with the predictable result: more towers, generators, and equipment sheds, but less resilient backhaul than is actually needed.

When cellular carriers and public safety organizations each build separately, the public gets the visual clutter and political cost of repeated tower siting fights, and responders still get dead zones.

A **neutral-host and co-location strategy** does not solve every problem, but it is the most transparent way to reduce redundant builds while improving coverage.

It starts with the basic work the state did not complete: a statewide inventory of dead zones, towers, shelters, backhaul, power, and ownership, and a map of where co-location is physically possible.

Absent those inventories, the state cannot honestly tell communities it has chosen the least-intrusive path to fill dead zones.

FirstNet does not cover gaps nor failover

FirstNet was conceived as a shared, interoperable public-safety broadband network.

In practice, it evolved into a single-carrier product riding on a commercial network that Vermont does not control and cannot adapt to resolve dead zones.

As a result, Vermont cannot rely on FirstNet alone to achieve resilient, statewide LTE coverage for first responders nor provide backup coverage when it fails, as it has repeatedly.

This reinforces, not weakens, the case for a state-supported, neutral-host infill strategy that avoids redundant towers, while enabling multi-carrier roaming and failover for eligible public-safety users.

The danger of premature statewide CAD

A computer-aided dispatch (CAD) system is a legitimate operational need. However, deploying it prematurely creates severe risks.

A statewide CAD system centralizes:

- Unverified narrative data
- Anecdotal officer notes
- Informal flags and comments

Absent strict, enforceable, auditable access controls—such as verified case numbers and legitimate purpose requirements—this data can be misused across jurisdictions.

Once centralized, this risk cannot be undone.

Moreover, CAD does not solve Vermont's most acute problems:

- Interoperability
- Failover
- Staffing resilience
- Coverage gaps
- Governance

CAD is **icing on the cake**. Vermont does not yet have a cake.

The Crosswinds/VALCOUR bind

The Department of Public Safety is approaching the end of a five-year contract with Crosswinds for the VALCOUR records management system (RMS). That system was originally expected to evolve into CAD. It will not.

There is now strong institutional pressure to:

- Extend the VALCOUR contract,
- Limit future CAD options to vendors interoperable with it,
- And justify that extension as benefiting "regional dispatch."

This risks spending scarce funds to prolong a system already acknowledged as inadequate, while foreclosing better long-term solutions.

A short, tightly limited extension may be unavoidable. A long-term recommitment would be a strategic error.

Corrective strategy: what should happen next

To provide robust public safety communications, Vermont needs statewide and regional governance, a pilot project(s), and a sustainable funding source.

1. Establish a new Communications Resilience and Public Safety Board

A new state dispatch board should be created, co-located with (but not replacing) the E-911 Board.

Its mandate would be limited and specific:

- Set standards for dispatch reliability, resilience, and training
- Support completion of the planning work required by Act 78
- Assure completion of the independent reviews required by 3 V.S.A. § 3303
- Oversee pilot project implementation and replicability
- Address privacy, access, and governance for statewide systems

Board membership must be independent, subject matter qualified, and not ceremonial.

2. Regional pilot: Washington–Caledonia Counties

Rather than attempting a statewide rollout, Vermont should implement a **proof-of-concept regional pilot**, pairing:

- Washington County, and possibly
- Caledonia County as a failover partner

This pilot would deliver **modular outputs** that other counties can reuse:

- Infrastructure inventories
- Coverage and dead-zone maps
- Land mobile radio and LTE/cellular in-fill strategies with resilient backhaul
- Governance
- Training and failover protocols and testing
- Cost and sustainable revenue models

This approach reflects real-world staffing, geography, and operational constraints.

3. Budget discipline and sequencing

Using the remaining **$9.5 million** (GF), the pilot would fund:

- Regional Planning Commission convening and GIS work: **$100–$200K**
- Independent engineering (LMR + LTE propagation, lifecycle): **$1.5–$2.0M**
- Privacy, data governance, and CAD policy analysis: **$0.5–$0.75M**
- Utility right-of-way inventory and revenue modeling: **$1.0–$1.5M**
- Limited physical anchor sites and proof points: **$3.0–$4.0M**

This remains within available funds and avoids premature build-out.

4. Revenue modeling, not wishful thinking

Vermont cannot rely indefinitely on grants.

A sustainable revenue model must be developed, including:

- Inventory of utilities occupying public rights-of-way
- Financial modeling of fair-market-value rent for use of rights-of-way
- Public Utility Commission oversight of cost allocation
- Transportation Fund implications for state highways
- Municipal revenue options for non-state rights-of-way

This work takes time, likely several years, but must begin now.

Why legislative action is required now

The history of Vermont's public safety projects demonstrates a consistent pattern:

- Fragmented authority
- Planning dismissed as "out of scope"
- Spending before analysis
- No accountable owner of end-to-end public safety communications

Agencies cannot correct this on their own. The Legislature must.

This report provides a path that:

- Completes work already paid for,
- Prevents another Lifeline/VCOMM-scale ($27 million) failure,Protects privacy and civil liberties,
- And creates infrastructure that can be sustained, not abandoned.

Conclusion

Vermont does not lack money because it lacks planning. It lacks planning because accountability has been diffuse and authority fragmented.

This corrective strategy restores sequence, discipline, and public trust. It does not delay progress. It makes progress real.

Chapter 1 – Why Course Correction Is Required

Vermont is not facing a minor delay or a problem of execution. It is facing a decision problem. The Legislature is being asked to move from planning to spending before the basic work that makes spending responsible has been finished. Course correction is required, not because modernization is unnecessary, but because proceeding now would lock the State into risk, cost, and weak governance for decades.

This is not about picking the right vendor or moving faster. It is about avoiding a pattern Vermont already knows: buying technology and committing money before the facts, authority, and sequence are clear.

The State Is at a Lock-In Point

Public safety communications systems last a long time. Once governance bodies are named, contracts signed, and equipment deployed, reversing course becomes politically and practically difficult. Early choices harden quickly. Even flawed systems persist because money has been spent, staff have adapted, and undoing the work looks disruptive.

The current recommendations are often described as incremental or reversible. They are not. Authorizing implementation funding, formalizing governance structures, or issuing major procurements would sharply narrow future legislative options. Those actions would commit Vermont to a specific order of decisions—governance, technology, and funding—before the prerequisites for informed choice are in place.

Course correction is required because the State is approaching this lock-in point without decision-quality information.

Legislative Direction Was Skipped, Not Completed

The Legislature did not create the Public Safety Communications Task Force togenerate ideas or justify early spending. Act 78 required specific foundational work: statewide inventories, real coverage analysis, evaluation of governance models, and a sequenced plan tied to accountability. These were not suggestions. They were statutory requirements.

That work was not completed. Inventories remain partial. Coverage analysis for land mobile radio and broadband LTE is incomplete and not usable for hard decisions. Governance authority at the regional level—where systems actually operate—remains undefined. Deadlines passed without formal acknowledgment or corrective direction, and later oversight requirements added through budget amendments were not fully integrated.

Accepting the current recommendations as a basis for implementation would invert legislative intent. It would treat statutory requirements as optional and compliance as flexible. Course correction is required to reassert that legislative direction is binding.

Uncertainty Is Being Carried Forward

The Task Force was meant to reduce uncertainty so that legislators could act with confidence. Instead, uncertainty has been documented and normalized.

Authoritative data already held by the State was not pulled together into a clear baseline. Coverage claims are hedged rather than verified. Sensitivity concerns are used to explain why analysis is missing instead of to protect details after analysis is done. Legislators are being asked to authorize major spending without knowing, in concrete terms, where systems fail, why they fail, or which fixes would actually work.

Proceeding under these conditions does not manage risk. It preserves it. Course correction is required because uncertainty has become an outcome of the process, not a problem the process solved.

Governance Has Been Pushed Too Far Downstream

Public safety communications are regional in practice. Dispatch centers serve multiple towns. Radio coverage crosses boundaries. Failover depends on shared systems. Vermont's experience shows that informal or advisory governance does not hold over time. Committees without real authority fade quietly and leave no one accountable when systems fail.

The current recommendations gesture toward governance but do not resolve it. Who has decision authority? Who enforces standards? Who resolves disputes?

Who is responsible when failover does not work? These questions are left unanswered, even as implementation is discussed.

Deploying technology before governance is settled creates brittle systems that rely on goodwill instead of enforceable responsibility. Once systems are live, governance debates become constrained by operational dependence. Course correction is required now to ensure that governance comes first.

Technology-First Sequencing Repeats Known Mistakes

Vermont has been here before. Radio systems and broadband initiatives were advanced before coverage was verified, ownership was clear, or long-term costs were understood. Systems were built, partially used, and later abandoned or retrofitted at high public expense.

The current trajectory risks repeating that pattern. Coverage targets are mentioned without defined performance conditions. Spectrum and backhaul feasibility are assumed rather than demonstrated. Ownership, maintenance, and replacement responsibility are left vague. Claims about resilience and failover are made without showing how they would actually work.

This is not a debate about whether certain technologies are promising. It is a recognition that technology-first planning fails predictably when analysis and governance lag behind. Course correction is required because the State already knows the outcome of this approach.

FirstNet is not a Substitute for State or Town Public Safety Communications Resiliency

It is tempting to treat FirstNet participation as a solution to Vermont's LTE coverage gaps. That is a mistake.

FirstNet does not give the State control over network architecture, siting priorities, reliability assurance, or carrier participation. It cannot be directed to fill Vermont's dead zones, and it cannot be used to rationalize where towers are built or shared.

Independent commentary on FirstNet's evolution confirms what Vermont agencies already experience operationally: the original vision of a shared, interoperable public-safety broadband network was displaced by a single-carrier

model that serves national business incentives, not local coverage optimization. Vermont can benefit from FirstNet subscriptions, but it cannot plan around them.

This reality makes planning more important, not less.

If Vermont proceeds with tower siting, LTE infill, or radio upgrades without a co-location-first and neutral-host discipline, it will trigger repeated local opposition while still failing to close dead zones.

A neutral-host approach—focused on shared towers, shared shelters, shared backup power, and resilient backhaul—reduces the number of structures required and creates the only credible path to multi-carrier failover for eligible public-safety users.

This is not a claim of new authority. Federal law limits state control over wireless safety concerns and certain siting outcomes. But Vermont's PUC retains leverage over tower sites, resiliency requirements (such as backup generators), and what conditions are attached to shared infrastructure. Ordering those choices transparently is the State's best defense against both technical failure and political backlash.

The State Is Paying for Past Infrastructure Choices Again

Backhaul is now cited as a major cost driver for public safety communications. That need did not appear out of nowhere. It is the result of broadband deployment that was never engineered to support public safety resilience.

Large sums were invested without requiring coordinated engineering, redundancy, or integration with emergency communications needs. The State is now being asked to fund parallel or supplemental infrastructure to achieve reliability that should have been built in from the start.

Treating this as unavoidable hides the underlying failure and risks locking in long-term fiscal exposure. Course correction is required before additional money is committed on the same fragmented basis.

Consultant Activity Has Replaced Planning Discipline

Consultants were meant to support the Task Force, not substitute for completion of required work. Instead, consultant deliverables were accepted with caveats,

known gaps were carried forward, and additional engagements were layered on without resetting the scope or enforcing outcomes.

The problem is not the use of consultants. It is the lack of enforceable, outcome-based requirements tied to statute. Effort has been treated as progress. Course correction is required to restore the distinction between activity and completion.

What Course Correction Means Now

Course correction does not mean abandoning reform or delaying indefinitely. It means stopping before irreversible decisions are made.

At this stage, course correction means insisting on completion of the work the Legislature already required:

- a comprehensive statewide inventory of assets;
- engineering-grade coverage analysis for land mobile radio and broadband LTE;
- defined regional governance with real authority and accountability; and
- a plan that ties funding to verified readiness.

These are procedural corrections, not ideological ones. They do not dictate outcomes. They restore the conditions under which outcomes can be chosen responsibly.

Proceeding without this correction would not be progress. It would be a decision to repeat known failures under the pressure of momentum. The Legislature still has the authority to insist on a different path. Using that authority now is not an obstruction. It’s stewardship.

Chapter 2 – Act 78: Required vs. Delivered

Why Act 78 Was Passed

Act 78 was not written to encourage exploration or to endorse gradual progress. It was passed to stop drift.

By the time the Legislature acted, Vermont's public safety communications system showed clear warning signs: dispatch centers operating in isolation, uneven land mobile radio coverage, growing dependence on commercial broadband that was never designed for emergency use, and no clear line of authority responsible for fixing any of it. The Legislature did not lack awareness. It lacked reliable information and enforceable structure.

Act 78 was meant to supply both. Its purpose was simple and corrective: give legislators decision-grade facts, clear options, and a sequence that preserved legislative control before money and technology locked the State into another generation of fragile systems.

What the Legislature Explicitly Required

Act 78 required completion of four connected pieces of work. Each was necessary on its own, and none could substitute for another.

1. A statewide factual baseline.
The Task Force was required to produce a comprehensive inventory of public safety communications assets across Vermont. That meant dispatch centers, radio systems, towers, backhaul, broadband dependencies, ownership, governance arrangements, age, condition, and known failure modes. This was not clerical. Without a baseline, legislators cannot tell whether money fills gaps or duplicates existing systems.

2. Real performance analysis.
The statute required analysis of how systems actually perform for responders in the field. For land mobile radio, that means coverage, capacity, and reliability under realistic conditions, including portable and in-building use. For broadband LTE, it means knowing where commercial networks work, where they do not, how they behave during congestion, and what happens when power or fiber fails. The goal was to replace assumptions with verified performance.

3. Governance evaluation.
The Legislature recognized that public safety communications are regional by function but fragmented by authority. Act 78 required examination of governance models capable of enforcing standards, assigning responsibility, resolving disputes, and sustaining systems over time. The Task Force was not asked to describe coordination challenges. It was asked to identify a structure that works.

4. A sequenced plan.
Finally, Act 78 required an ordered path forward. Governance before procurement. Analysis before investment. Pilots before scaling. Funding tied to readiness. Sequencing was the safeguard that kept early decisions from becoming irreversible mistakes.

These requirements were not optional. They were designed to prevent exactly what Vermont has experienced before: spending first and discovering consequences later.

What Was Actually Delivered

The Task Force delivered activity, not completion.

Meetings were held. Consultants were engaged. Issues were catalogued. What was not delivered was the decision-enabling foundation Act 78 required.

There is no comprehensive statewide inventory that allows a legislator to answer basic questions: how many dispatch centers exist, what systems they use, who governs them, how old they are, and who is responsible when they fail. Information appears in fragments, but it is not assembled into a usable baseline.

Coverage analysis is incomplete and not suitable for hard decisions. Broadband LTE discussion relies heavily on limited drive testing along major roads, despite acknowledging that responders do not operate only on highways. Cellular antenna data already held by the State's 911 system was not fully integrated. As a result, broadband is discussed in terms of promise and variability rather than verified reliability.

Land mobile radio analysis is thinner still. The record acknowledges uneven coverage and aging systems but does not provide a statewide, engineering-grade assessment. Claims of public records exemption due to sensitivity are used to explain why analysis is missing, even though such analysis is routine for operating systems elsewhere.

Governance analysis remains conceptual. The Task Force recognizes that governance matters but does not define where binding authority would reside, how standards would be enforced, or how disputes would be resolved. Vermont's long history of advisory regional bodies that lack real power is noted but not corrected.

Most importantly, no sequenced plan was delivered. Technology concepts appear before governance is settled. Cost discussions appear before performance is established. Funding pathways are discussed before ownership and accountability are defined. This reverses the order Act 78 was meant to enforce.

Missed Deadlines and Silent Noncompliance

Act 78 included deadlines because time is not neutral in this domain. Systems continue to age. Risks accumulate. Leverage over cost and design declines.

Those deadlines were missed. More concerning than the delay is how it was treated. Noncompliance was not formally acknowledged. Corrective direction was not sought. Work continued as if statutory timelines were flexible rather than binding.

If foundational planning requirements can lapse without consequence, future corrective legislation loses force. Oversight becomes ceremonial rather than corrective.

From Planning to Promotion

Over time, the character of the Task Force's work shifted.

Analysis was supposed to narrow options and force tradeoffs. Instead, recommendations are framed as an "important beginning." That language matters. A beginning invites momentum. Act 78 required clarity.

Describing unfinished work as a starting point asks legislators to fund movement rather than decisions. It substitutes optimism for completion. That framing is incompatible with the statute's purpose.

This is not a dispute over which technologies or models might eventually make sense. It is a failure to complete the work needed to justify any choice at all.

Why the Gap Matters

Public safety communications systems fail quietly until they fail catastrophically. When responders cannot communicate, there is no workaround.

Planning errors made today persist for decades because radio systems, dispatch architectures, and governance arrangements are expensive and politically hard to unwind. When the State commits without understanding performance, cost, and authority, it locks itself into retrofits, workarounds, and repeated spending.

Technical dependencies amplify this risk. Land mobile radio, broadband LTE, fiber backhaul, dispatch software, records systems, and cybersecurity controls are tightly linked. Decisions in one layer constrain options in others. Without a completed baseline and enforced sequence, Vermont cannot know whether it is building a coherent system or stacking incompatible parts.

What This Chapter Establishes

This chapter does not propose solutions. It establishes a record.

Act 78 required decision-grade planning. What was delivered does not meet that standard. The gap is not about effort or intent. It is structural.

Until the Legislature has the inventories, verified performance analysis, defined governance with real authority, and a sequenced plan tying funding to readiness, it does not have a responsible basis for authorizing major implementation spending.

That conclusion is not aggressive. It is simply faithful to what the statute demanded.

Chapter 3 – Act 87, Section 49: Budget Adjustment and the Failure of Unified Oversight

Why This Chapter Exists

This chapter examines a narrow but decisive legislative intervention that occurred after Act 78 was enacted and while the Public Safety Communications Task Force was still operating.

Act 87 is a wide-ranging budget adjustment act covering hundreds of unrelated subjects. This chapter is not about Act 87 as a whole. It focuses solely on Section 49, because that section represents the Legislature's explicit attempt to impose oversight at a moment when public safety communications spending was moving faster than planning, governance, and sequencing could support.

Section 49 was not an afterthought. It was enacted because the Legislature recognized that once federal and state funds are spent on radios, dispatch infrastructure, backhaul, or vendor contracts, those decisions shape the system for decades. This chapter explains what Section 49 was intended to do, how it depended on Act 78 planning, and why it failed to operate as a real corrective brake.

What Act 87, Section 49 Actually Did

Section 49 did not create a new program, governance body, or procurement authority. It worked within the budget to place conditions and expectations on funds already in motion.

First, Section 49 explicitly tied approximately $9 million in Congressionally Directed Spending administered through the Department of Public Safety to the statewide public safety communications system under development. This linkage mattered. The Legislature understood that these funds would influence radio systems, dispatch infrastructure, backhaul, and vendor relationships long after the budget year closed.

Second, Section 49 required coordination and visibility rather than command. The Commissioner of Public Safety was directed to coordinate federal expenditures with the statewide system, inform the Task Force as spending parameters became available, solicit Task Force recommendations regarding plans, schedules, and expenditures, and provide updates to the Joint Fiscal Committee.

Section 49 required an ongoing, bidirectional information flow with the Public Safety Communications Task Force, as federal parameters evolved and as expenditure plans were revised.

Based on review of available Task Force minutes and meeting transcripts, and informal inquiry to Task Force members, it is unclear whether updated information regarding extensions, obligation status, or revised expenditure timelines for the congressionally directed funds was shared with the Task Force after initial discussions.

If such information was not shared, Task Force deliberations and recommendations would necessarily have proceeded without the full and current context required by Act 87.

Such uncertainty underscores the need for explicit, auditable reporting checkpoints and shared visibility into funding status and sequencing, as proposed in this report.

Third, Section 49 assumed that Act 78 planning would be complete or nearly complete. It did not restate inventory, coverage analysis, governance evaluation, or sequencing requirements because those obligations already existed. Section 49 relied on the Task Force's ability to provide decision-grade advice about whether federal spending aligned with a coherent statewide and regional architecture.

Section 49 was designed to slow spending just enough to allow planning to catch up. It was a corrective pause, not a green light.

What "Unified Oversight" Was Supposed to Mean

Unified oversight in Section 49 did not mean centralizing operations or eliminating regional control. It meant forcing planning, funding, and accountability to meet before irreversible commitments were made.

In practical terms, unified oversight required someone to be able to answer basic questions before money moved:

- Would a proposed radio or dispatch investment lock the State into a governance model that had not been chosen?
- Would broadband or fiber spending create vendor or backhaul dependencies that undermined resilience?
- Would early procurement narrow options for shared dispatch, records systems, privacy controls, or cybersecurity enforcement?

Section 49 existed to make sure those questions were asked while answers still mattered.

What Did Not Happen

The Task Force's final work does not meaningfully document how Section 49 was carried out.

There is no clear accounting of how Congressionally Directed Spending was coordinated with statewide planning. There is no record of substantive recommendations shaping plans, schedules, or expenditures. There is no explanation of how Task Force input constrained, redirected, or delayed spending decisions. Updates to the Joint Fiscal Committee are not tied back to concrete oversight outcomes.

Federal funds are referenced as a resource, but not situated within the oversight structure Section 49 created. As a result, the Legislature cannot tell whether its corrective intent was fulfilled or bypassed.

This is not a matter of tone or documentation style. Without evidence of how Section 49 functioned in practice, unified oversight collapses into reporting without control.

Acting Without the Planning Foundation

Section 49 assumed that Act 78 planning would provide a stable foundation for coordination. That assumption proved false.

As established elsewhere, statewide inventories were incomplete. Coverage analysis for both land mobile radio and broadband LTE was partial and not decision-enabling. Regional governance authority remained undefined. Technical dependencies among radio systems, broadband, fiber backhaul, dispatch platforms, records systems, and cybersecurity controls were unresolved.

Without those foundations, coordination became hollow. Recommendations could not be grounded in verified performance, lifecycle cost, or governance reality. Federal spending advanced without a clear understanding of whether it supported or constrained future statewide and regional systems.

This is how mis-sequencing hardens. Once equipment is installed or contracts are signed, later governance and architecture choices narrow rapidly. Section 49 was meant to prevent that outcome.

Why the Failure Matters

Budget adjustment acts are used precisely because timing matters. Section 49 was enacted because the Legislature understood that oversight after procurement is too late.

When coordination is deferred, fragmentation becomes permanent. Radio systems are built without clear ownership. Broadband dependencies are assumed rather than engineered. Dispatch and records systems evolve without unified access control or auditability. Cybersecurity risk grows as systems interconnect without baseline standards.

Section 49 was a targeted legislative tool designed to interrupt that pattern. Its failure to produce visible, enforceable oversight increased long-term cost and risk, even if individual expenditures had operational value.

What This Chapter Does — and Does Not — Claim

This chapter does not allege misuse of funds or bad faith by agencies or individuals. It does not claim that Congressionally Directed Spending lacked public safety benefit.

It identifies a governance failure.

The Legislature amended the budget to impose coordination, visibility, and sequencing discipline. The structure relied upon to provide that discipline did not document how it was exercised. As a result, legislative oversight could not function as designed.

Why Section 49 Cannot Be Treated as Incidental

Section 49 was not surplus language. It was an explicit signal that the Legislature recognized emerging risk and attempted to correct course midstream.

If a targeted budget amendment tying federal funds to statewide planning can be treated as background rather than binding, future corrective interventions will carry little weight. The issue is larger than this section alone. It is whether legislative efforts to slow, align, and protect public investment are respected in practice.

What This Chapter Establishes

This chapter does not propose remedies. It establishes a record.

The Legislature acted through Act 87, Section 49 to impose unified oversight at a critical moment. That oversight did not translate into documented, decision-shaping outcomes. Recognizing that failure is necessary before additional authority, funding, or system expansion is considered.

Without that recognition, reform will follow the same pattern again: planning deferred, money spent, and accountability postponed.

Chapter 4 – Fragmented Authority and Deniability

The Problem Addressed in This Chapter

Vermont's public safety communications problems are often blamed on technology, funding, or staffing. Those problems are real. They are not the root cause.

The deeper issue is structural. Authority is spread across too many actors, at too many levels, with no one clearly responsible for whether the system works when it matters. When something fails, every participant can plausibly say it was not their decision to fix.

This chapter explains how that fragmentation operates, why it produces deniability instead of correction, and why failure under stress is predictable under the current structure.

Fragmentation by Design, Not Accident

Public safety communications are regional by nature. Dispatch centers serve multiple towns. Radio coverage crosses municipal and county lines. Mutual aid depends on shared systems and shared rules.

Vermont's governance structure does not match that reality.

Local governments retain control over dispatch operations and radio use, but lack the scale and capacity to plan, fund, and sustain modern systems. Regional groupings exist on paper, but most lack staff, budget authority, or power to make binding decisions. State agencies fund equipment, offer technical support, or set limited standards, but do not take responsibility for end-to-end system performance.

Each layer can point elsewhere. Towns point to the state for funding. The state points to local control. Regional bodies explain that they can only advise. When problems persist, responsibility dissolves because it was never clearly assigned.

This structure did not emerge by accident. It is the result of repeated choices to add programs and committees without deciding who owns the outcome.

Advisory Bodies Without Consequences

Vermont relies heavily on advisory groups. Task forces, boards, and committees study problems, hold meetings, and issue recommendations. They do not have the authority to require action.

When recommendations are ignored, nothing happens. When deadlines pass, nothing happens. When required analysis is unfinished, new studies are commissioned instead of gaps being closed.

This creates institutional cover. Agencies can say they participated. Officials can say they reviewed the work. Everyone can point to process. No one is accountable for results.

For legislators and local officials, this is dangerous. A report on a shelf looks like progress. In practice, it often signals that no one had the authority to decide.

Regional Responsibility Without Regional Power

Dispatch and radio systems operate at a regional scale. Governance does not.

Many dispatch centers are formed through inter-municipal agreements. On paper, they create boards or committees. In practice, many meet irregularly, avoid hard decisions, and lack basic powers. They cannot set rates, require participation, enforce standards, or compel long-term commitments.

When disagreements arise, withdrawal becomes the only real option. That reality shapes behavior. Towns hesitate to invest because they cannot control what neighbors will do. Costs are deferred because no one can impose them fairly. Standards vary because adoption is voluntary.

The Task Force record acknowledges the need for regional coordination but does not define a regional authority capable of governing. Responsibility without power is not responsibility. It is exposure.

State Involvement Without State Accountability

Several state agencies touch public safety communications. One manages funding. Another supports emergency services. Another operates the 911 system. Each controls a piece.

No one owns the whole.

Agencies may buy radios without controlling how they are used. They may support broadband access without ensuring it functions during storms. They may issue guidance without enforcing it. When failures occur, responsibility slides downhill to towns or sideways to another department.

This allows good-faith participation without outcome accountability. That is deniability built into the system.

Oversight That Cannot Correct

Statutes require reports, updates, and oversight. Those tools only matter if they have consequences.

In the current structure, they do not. Deadlines pass without explanation. Required analysis remains unfinished. Funds move while core questions remain unanswered. Oversight becomes a record of uncertainty rather than a trigger for correction.

No single entity is required to certify that planning is complete before money moves. No one is empowered to stop a project that is out of sequence. Oversight exists, but it has no teeth.

The Asymmetry Between 911 Resilience and Dispatch Failure

One contrast makes this risk concrete.

Inbound 911 calls in Vermont are engineered to fail over. If one answering center goes down, calls can route to another. Authority is clear. Funding is stable. Rules are enforced. The system works, even if imperfectly.

Dispatch does not operate that way.

Dispatch systems are tied to specific centers. Consoles, talk groups, access permissions, and staffing are local. If a center loses power, staff, or connectivity, nearby centers cannot simply take over. They lack pre-set access, legal authority, staffing plans, and funding agreements.

This creates a dangerous asymmetry. Vermont can receive emergency calls while being unable to coordinate response. During a major storm or regional outage, that gap becomes critical.

The risk is amplified because dispatch systems often share power sources, towers, and fiber routes with the radio systems they depend on. Failures cascade. They do not stay isolated.

This is not hypothetical. It is a foreseeable outcome of fragmented governance.

Consultants as a Buffer, Not a Solution

Consultants appear repeatedly in this structure. They are hired to study problems, analyze options, and facilitate discussion.

When their work falls short, responsibility blurs. Agencies say they relied on expert advice. Consultants say they worked within scope. Task forces say they reviewed what was provided.

The result is activity without ownership. Reports without decisions. Process without accountability.

This is not a critique of consultants. It is a warning about how they are being used. When no one has authority to decide, consultants become a buffer rather than a tool.

Fragmentation Produces Risk

Fragmented authority is not just inefficient. It is dangerous.

Public safety systems are stressed by storms, staffing shortages, cyber incidents, and multi-agency events. When authority is unclear, response slows. When governance is informal, failover breaks down. When no one owns the system, vulnerabilities persist.

These risks compound over time. Infrastructure ages. Institutional memory drains away. Each delay raises the cost and difficulty of correction.

Public trust erodes as well. Responders know the systems are fragile. Communities are told progress is being made. When failures continue, confidence drops because no one appears responsible.

Why the Pattern Persists

This structure persists because it is comfortable.

Clear authority creates clear responsibility. Clear responsibility creates accountability when things go wrong. Fragmentation allows progress to be claimed without owning results.

Local control can be defended even when local capacity is insufficient. State involvement can be cited without state accountability. Advisory groups can be praised without being empowered.

Everyone participates. No one decides.

Why Legislative Action Is Required

This problem cannot resolve itself. Agencies can only act within the authority they have. No agency can consolidate power it does not possess.

Only the Legislature can decide where authority belongs and make that authority real. That means naming who is responsible for system performance, tying funding to accountability, and replacing advisory roles with governing ones where systems demand it.

This is not about centralization for convenience. It is about matching authority to function.

The Cost of Avoiding the Issue

Avoiding this question has a price. It appears as repeated studies, stalled projects, uneven service, and growing operational risk. It also appears as public money spent without durable results.

Every new task force that leaves authority fragmented extends the problem. Every appropriation made without resolving governance deepens the lack of responsibility and accountability.

The choice is simple. Continue funding activity within a structure that allows deniability, or insist on a structure that makes accountability unavoidable.

This chapter exists to make that choice clear.

Chapter 5 – Statewide Governance Architecture

Why Statewide Structure Matters

Public safety communications only work when someone owns the whole system. Not pieces. Not studies. The whole thing.

Vermont does not have that today.

Local governments operate dispatch. Regions try to cooperate without formal governance. State agencies maintain parts of the system and set limited rules. No one is responsible for whether the system works end to end—during a storm, a staffing collapse, or a prolonged outage. That gap is not accidental. It is built into how authority is divided.

This chapter explains why statewide governance is necessary, what it must do, and what it must not pretend to do. The goal is simple: one clear place where responsibility for system performance lives, paired with empowered regional operators who can make the system work day to day.

What Statewide Governance Is — and Is Not

Statewide governance is not about running dispatch from Montpelier. It is not about micromanaging towns. It is about setting and enforcing the rules that make a statewide, regional system possible.

A simple comparison helps. The state sets highway standards. Towns plow local roads. No town can decide to ignore bridge safety rules. No agency can claim a collapsed bridge is not its problem. Public safety communications require the same clarity.

Statewide governance defines what “works.” It sets conditions that must be met before money moves or equipment is installed. It enforces order so early decisions do not lock in failure.

Statewide governance cannot replace regional authority. Dispatch operations, radio coverage, staffing realities, and failover execution are regional by nature. Pretending a statewide body can run those operations directly creates delay and blame-shifting. The state must set the frame and enforce it. Regions must operate within that frame with real authority.

What the State Must Own

There are decisions that cannot be left to voluntary agreement. The state must own them.

System standards.
The state must define minimum standards for radio coverage, dispatch availability, failover expectations, records retention, privacy controls, and cybersecurity. Optional standards are ignored when budgets tighten. Required standards protect responders and the public.

System architecture.
Land mobile radio, commercial broadband, fiber backhaul, dispatch software, records systems, and security controls depend on each other. If each layer is chosen in isolation, the result is a fragile stack. The state must define how the pieces fit together before regions or towns buy parts.

Sequencing.
Governance must come before procurement. Coverage must be verified before expansion. Failover must be engineered before consolidation. When money moves out of order, mistakes become permanent.

Accountability.
Someone must be able to say yes or no. Someone must certify that prerequisites are met. Someone must be answerable when systems fail. Without that authority, oversight is symbolic.

What the State Must Not Pretend to Do

Statewide governance cannot do everything, and pretending otherwise creates false confidence.

The state should not promise operational control it cannot exercise. When statewide bodies issue guidance without enforcement power, towns assume someone else is in charge. The public assumes someone is watching. No one is.

Statewide governance must be limited to what the state can actually enforce: standards, sequencing, funding gates, and accountability. Operations belong with regions that have staff, facilities, and local knowledge.

The Missing Link Between State and Region

Today, the state talks to towns. Regions are treated as optional. That is backwards.

A statewide system requires regional operators with real authority. Those regional bodies need legal standing, control over shared infrastructure, and stable funding. The state's role is to require that structure and recognize it in law.

Without that link, statewide governance becomes advisory. Regions drift. Towns opt out. Systems fragment again.

Funding Without Architecture

Vermont has a long history of funding equipment before deciding who will own it, maintain it, or replace it.

A radio grant buys radios. It does not guarantee coverage.
A broadband grant buys access. It does not guarantee resilience.
A dispatch upgrade buys software. It does not guarantee failover.

Statewide governance must tie funding to architecture. No money should move unless it supports a defined system with defined owners and defined obligations. Grants without architecture create stranded assets.

Revenue and Cost Responsibility

Operating costs last longer than grants. Dispatch salaries, radio maintenance, data storage, security updates, training, and replacement cycles continue year after year.

Statewide governance must require clear cost responsibility before systems expand. Towns must know what they will owe over time. Regions must be able to set rates and collect revenue. If costs are hidden or deferred, participation erodes and corners get cut.

The state does not need to pay every bill. It must require that every bill has an owner.

Legal Authority and Enforcement

Rules without enforcement are suggestions.

Statewide governance must have clear legal authority to set standards and require compliance. That includes the power to block funding when prerequisites are not met, to require interoperability and failover agreements, and to demand corrective action when audits or incident reviews reveal failure.

Without enforcement, statewide governance becomes another committee. Vermont already has enough of those.

Technology Is Not the Hard Part

Radios work. Fiber works. Dispatch software works.

The hard part is deciding who controls these tools and how they are used together. Cybersecurity makes this urgent. As dispatch, records, radio, and broadband systems connect, risk increases. A weak password in one town can expose a region. A misconfigured server can disrupt dispatch across counties.

Statewide governance must require baseline security controls and compliance. Leaving this to voluntary practice is reckless.

A Concrete Failure Scenario

Consider a winter storm that knocks out power and fiber to a regional dispatch center. Calls still route through 911 failover. Dispatch cannot move. Neighboring centers want to help but lack access, authority, staffing plans, or funding agreements. Radios work in some areas and not others. No one knows who is in charge.

In that moment, governance matters more than technology. If authority is clear, systems switch. If it is not, confusion fills the gap.

Why This Cannot Be Optional

Voluntary coordination has failed. Advisory boards have failed. Pilot projects without structure have failed.

Statewide governance is not a preference. It is a requirement if Vermont wants a public safety communications system that works under stress. That governance must be real, limited to what the state can enforce, and paired with empowered regional operators.

The Cost of Getting This Wrong

If statewide governance is weak, every other reform is fragile. Money will be spent. Systems will be built. Failures will continue. Blame will circulate.

If statewide governance is clear, fewer projects will move quickly. That is the point. Speed without structure is how Vermont got here.

This chapter exists to make one thing plain. Without a real statewide governance architecture that sets rules, enforces sequence, and assigns responsibility, no amount of technology or funding will deliver a reliable public safety communications system.

Chapter 6 – Regional Governance and Failover

Why the Regional Layer Matters

Public safety communications do not work town by town. They work across regions.

Dispatch centers serve multiple municipalities. Radio coverage crosses county lines. Mutual aid depends on shared systems. When something breaks, the failure spreads. Vermont talks about regional systems, but it does not govern them. That gap explains why failover is weak, costs drift, and responsibility blurs.

This chapter explains what regional governance must do, why it must be real, and why failover fails without it. Statewide rules matter, but systems succeed or fail where regions operate.

What Regional Governance Must Control

A regional authority must be able to decide—not advise.

It must control participation. If a town uses the regional system, it must follow the rules and pay its share. Drifting in and out cannot be an option.

It must control shared infrastructure. Radios, towers, fiber backhaul, dispatch consoles, records systems, and security controls need a clear owner who answers for uptime, maintenance, and replacement.

It must control operating standards. Staffing levels, training, call handling, radio discipline, and security practices cannot be optional or left to local habit.

It must control money. Rates must be set. Bills must be paid. Reserves must be built. Grants cannot be treated as free money that hides long-term costs.

Without these powers, a regional body is a discussion group. Vermont already has many of those.

Failover Is a Governance Problem First

Failover sounds technical. It is not. It is a promise.

Failover means that when one dispatch center cannot operate, another will take over.

That promise only holds if three questions are answered in advance:

1. Who must take the calls and radio traffic—and for how long?
2. Who pays for the added staffing and operating cost?
3. Who decides when failover starts and when it ends?

In Vermont, these questions are usually unanswered. Centers help each other informally during short events. That does not scale to long outages, staffing collapses, or regional storms.

Without binding agreements, no center can be expected to absorb another center's workload for days or weeks. Without authority, no one can require it. Without funding, no one can sustain it.

What Happens When Regional Authority Is Weak

When regional governance is weak, the same failures repeat.

Systems are built without clear owners. Maintenance is deferred. Upgrades are uneven. Costs are argued town by town. Disputes stall progress.

Failover plans exist on paper but fail in practice. Access permissions are missing. Radio talk groups are not shared. Dispatch consoles are not configured. Staff are not trained to cover unfamiliar areas.

The public does not see these failures until something goes wrong. Then everyone is surprised, even though the warning signs were obvious.

The 911 Contrast Makes the Risk Clear

Inbound 911 calls in Vermont are designed to fail over. If one answering center goes down, calls route to another. That works because authority is clear, funding is stable, and rules are enforced.

Dispatch does not have that structure.

Calls can arrive. Help cannot move.

This contrast is not academic. It shows what happens when governance exists for one layer of the system and not the other.

Technology Cannot Fix Missing Authority

Mirrored servers, backup radios, and extra fiber do not solve failover if governance is missing.

A neighboring center cannot dispatch another region if it lacks legal authority, access to records, radio control, or a staffing plan. A spare console does nothing if no one is authorized or funded to use it.

Failover must be designed into operations, not bolted onto equipment.

Funding Must Follow Authority

Regional systems cost money every year: dispatch salaries, radio maintenance, data storage, security updates, and training.

Grants help with startup. They do not pay the bills forever.

Regional governance must be able to set rates and collect revenue. Towns must know what they owe and why. If costs are hidden or delayed, participation erodes and corners get cut.

The state should not promise savings from consolidation unless it also requires the governance needed to realize them. Without authority, consolidation often costs more, not less.

Legal Standing Cannot Be Optional

Regional bodies need clear legal standing. They must be able to sign contracts, hire staff, enforce agreements, and survive political turnover.

Handshake agreements fail when budgets tighten or leadership changes. Regional governance must outlast elections and personalities.

The state's role is to require this structure and recognize it in law. Without that backing, regions cannot govern.

Cybersecurity Raises the Stakes

As dispatch, records, radio, and broadband systems connect, risk increases. A weak password in one town can expose a region. A compromised server can disrupt dispatch across counties.

Regional governance must enforce baseline security rules and incident response. Leaving this to voluntary practice invites failure.

A Real-World Failure Scenario

Picture a prolonged ice storm. Power fails. Fiber lines drop. A regional dispatch center goes dark.

Calls still come in. Radios still work in some places. Neighboring centers want to help. They cannot. They lack access, authority, staffing plans, and funding to take over.

That is not a technology failure. It is a governance failure.

Why Regional Governance Cannot Be Advisory

Voluntary cooperation works on good days. Public safety systems must work on bad ones.

Advisory models assume goodwill. Failover requires obligation.

Regional governance must be mandatory where systems are shared. That is not heavy-handed. It is prudent.

How State and Region Must Fit Together

The state must set the rules. Regions must run the systems.

If the state tries to operate dispatch from afar, it will fail. If regions are left to self-organize without power, they will fail.

The line is clear. Statewide authority sets standards, sequencing, and enforcement. Regional authority owns operations, failover, and cost allocation within that frame.

The Cost of Avoiding This

Without real regional governance, every investment is fragile. Money will be spent. Systems will be built. Failover will be promised. Failure will persist.

With real regional governance, fewer projects will move quickly. More will work when they are needed.

This chapter exists to make one point unavoidable. Failover is not optional. Regional governance is not optional. One cannot exist without the other.

Chapter 7 – Governance Competencies and Appointments

Why People Matter as Much as Structure

Governance charts do not make decisions. People do.

Vermont's public safety communications problems are often framed as gaps in authority or funding. Those gaps matter. But even a well-designed structure will fail if the people appointed to govern it lack the skills, experience, or mandate to act.

This chapter explains why governance competence is not optional, what kinds of expertise are required, and why appointment practices must change if reform is to succeed.

Governance Is Skilled Work

Serving on a governing body for a public safety communications system is not ceremonial. It requires judgment under uncertainty, comfort with technical tradeoffs, and willingness to make unpopular decisions.

A governing board must be able to understand why a radio system fails in certain terrain, why broadband cannot substitute for land mobile radio, why failover requires staffing as well as equipment, and why cybersecurity failures cascade across systems.

Without that understanding, boards defer. They ask for more studies. They accept optimistic assurances. Delay becomes the default.

Competence does not require everyone to be an engineer. It does require enough technical literacy to know when questions are unanswered and when risks are being downplayed.

The Cost of Representative-Only Appointments

Vermont often fills boards to ensure geographic or stakeholder representation. Representation matters. On its own, it is not enough.

Boards composed entirely of representatives—town officials, agency designees, or interest group members—tend to defend local positions rather than govern the

system as a whole. Decisions stall because members are accountable to constituencies, not outcomes.

Public safety communications governance requires a different balance. Representation must be paired with expertise and independence. Otherwise, the board becomes a forum for negotiation rather than a body capable of enforcing standards.

Which Competencies Are Required

Effective governance requires specific competencies. They cannot be assumed.

Operational understanding.
Members must understand dispatch operations, staffing realities, and what happens during outages or major incidents. Governance divorced from operations produces fragile plans.

Technical literacy.
Boards must grasp the basics of radio coverage, broadband limits, backhaul dependency, and cybersecurity risk. This allows them to test vendor claims and consultant recommendations.

Financial judgment.
Lifecycle cost matters more than purchase price. Governing bodies must understand operating budgets, replacement cycles, and the difference between one-time grants and ongoing obligations.

Legal and accountability awareness.
Privacy law, labor rules, procurement limits, and liability exposure shape what is possible. Boards must know when informal practice crosses legal boundaries.

No single member needs all these skills. The board collectively must.

Appointments Signal Authority

Who is appointed tells everyone how seriously governance is meant to function.

When appointments are made as a courtesy or political accommodation, staff and vendors notice. When boards are filled with people who cannot say no, the system drifts.

Appointments must signal that the governing body has real authority and expects to use it. That means appointing people who are comfortable enforcing standards, delaying spending, and rejecting proposals that are out of sequence.

The Role of Independence

Governance fails when everyone at the table is dependent on someone else for budget, employment, or political support.

Independent members—people not directly tied to a single town, vendor, or agency—provide ballast. They ask questions others avoid. They focus on system performance rather than local impact.

Independence does not mean lack of accountability. It means freedom to govern in the public interest rather than negotiate on behalf of a seat.

Why Training Matters

Even well-chosen boards fail without support.

Governance members should receive structured onboarding. Not a binder. Real orientation covering system architecture, known risks, statutory obligations, and decision authority.

Ongoing training matters as well. Technology evolves. Threats change. New members join. Treating governance as a static role invites decay.

Training is not overhead. It is insurance.

Consultants Cannot Replace Governance

Consultants advise. They do not decide.

When boards lack confidence or competence, consultants fill the vacuum. Their recommendations become de facto policy because no one feels equipped to challenge them.

That dynamic shifts responsibility away from appointed governors and toward paid advisors. When outcomes disappoint, blame becomes diffuse.
Strong governance uses consultants as tools, not crutches.

A Predictable Failure Pattern

The pattern is familiar.

A board with limited technical literacy receives a report. The report flags risks but recommends moving forward. Members are uneasy but lack the grounding to push back. Funding deadlines loom. The board approves the plan “with conditions.”

Those conditions are never enforced. The system is built. Problems surface later. The board expresses concern and commissions another study.

This is not bad faith. It is predictable failure caused by weak governance capacity.

Why Appointment Reform Is Urgent

Public safety communications systems are becoming more complex, not less. Integration increases risk. Cyber threats grow. Staffing pressures rise.

Governance that could muddle through twenty years ago cannot manage what is coming next. Appointments must reflect that reality. Competence, independence, and authority must be explicit criteria, not incidental qualities.

The Legislature’s Responsibility

Only the Legislature can insist that governance appointments match responsibility.

That does not mean dictating who serves. It means setting expectations: required competencies, balanced composition, real authority, and accountability for outcomes. If appointments remain symbolic, reform will remain fragile.

What This Chapter Establishes

This chapter does not name individuals or prescribe appointment formulas. It establishes a principle.

Public safety communications governance is not a volunteer exercise. It is skilled work with real consequences. If boards are not built to do that work, no amount of structure, funding, or technology will compensate.

Getting governance right means getting the people right.

Chapter 8 – Cybersecurity and Incident Auditing

Why This Chapter Exists

Public safety communications now run on networks. Dispatch, radios, records, and broadband are connected. That connection brings speed and reach. It also brings risk.

When systems fail or are breached, the result is not an inconvenience. Calls stack up. Dispatch stalls. Records disappear. Trust collapses. Treating cybersecurity as a technical detail rather than a governance duty leaves the State exposed.

This chapter explains why cybersecurity and incident auditing must be governed as core public safety functions, not bolted on later.

Cyber Risk Is Already Here

This is not a future problem.

Dispatch relies on internet-connected software. Records systems store sensitive data. Radio controllers are networked. Fiber routes share poles and trenches with commercial traffic. Remote access is common because staffing is thin.

Each connection is a door. Some are locked. Some are not. Today, no one can say with confidence which is which across the State.

Cybersecurity Is Not an IT Problem

Cybersecurity fails when it is treated as an information technology task instead of a governance responsibility.

Technical staff can patch systems. They cannot decide risk tolerance. They cannot enforce standards across regions. They cannot stop a project that skips basic safeguards.

Only governance can do that.

A governing body must decide what level of risk is acceptable, what controls are mandatory, and what happens when controls are ignored. Without those decisions, security becomes optional and uneven.

Interconnection Raises the Stakes

Older public safety systems were isolated. New ones are not.

When dispatch connects to records, a breach exposes personal data. When dispatch connects to radios, an attacker can disrupt response. When broadband links field devices, outages and attacks can blind responders.

Each connection multiplies impact. A weak link in one town can expose a region. A misconfigured server can affect multiple agencies.

Voluntary security practices do not work in this environment. Risk does not respect boundaries.

A Simple Failure Example

Consider a phishing email sent to a dispatcher. A link is clicked. Malware enters the system.

If networks are flat and controls weak, dispatch software locks up. Radio control stalls. Records become inaccessible. Neighboring centers cannot help because systems are linked but not segmented.

This pattern is common elsewhere. The only question is whether Vermont is prepared. Right now, it is not.

Cybersecurity Depends on Basic Hygiene

Good security starts with simple steps: strong passwords, multi-factor login, segmented networks, regular updates, and backups that are tested—not assumed.

These steps cost money and time. They also require consistency.

If one center skips them to save money, the whole system is at risk. That is why governance must require them.

Cybersecurity Without Auditing Is Guesswork
Security claims mean nothing without verification.

Incident auditing answers basic questions after something goes wrong: What failed? Why? How long did it last? Who knew? What was done?

Vermont lacks a consistent audit framework for public safety communications incidents. Outages are handled locally. Lessons are not shared. Patterns are missed.

Without auditing, the same failures repeat quietly until they become public.

Auditing Is Not Blame

Incident auditing is often resisted because it is seen as punitive. That is a mistake.

Auditing is about learning. It is how aviation improved safety. It is how utilities improve reliability. It is how systems get better.

Without it, organizations guess. To guess in public safety is dangerous.

What Governance Must Require

Cybersecurity and auditing cannot be voluntary.

Governance must require baseline security controls across dispatch, radio management, records systems, and broadband access. It must require regular testing and independent review. It must require incident reporting and post-incident analysis.

These requirements must apply statewide and regionally. If one center opts out, everyone pays the price.

Funding Must Match Requirements

Security costs money. Firewalls, backups, monitoring, training, and audits are not free.

If the State mandates security without funding, compliance will be uneven. If it funds systems without mandating security, risk will grow.
Funding and requirements must move together. Grants should require proof of controls. Operating budgets must include security as a core cost, not an add-on.

The Role of the State

The State must set minimum security standards and require compliance. It must define what incidents must be reported and how audits are conducted. It must protect sensitive details while still enforcing accountability.

The State should not run local networks. It should enforce the rules that keep them safe.

The Role of Regions

Regional operators must implement controls, monitor systems, and respond to incidents. They must share lessons across the region and adjust practices when failures occur.

This only works if regions have real authority and stable funding. Security cannot depend on goodwill.

Cybersecurity Is a Public Safety Issue

When systems go down, responders lose information. Calls stack up. Dispatchers improvise. Mistakes happen.

Cybersecurity failures harm people, even when no one intends them to.

That is why this chapter treats security and incident auditing as core public safety functions, not technical add-ons.

The Cost of Avoidance

Ignoring this issue saves money today. It costs more later.

A single breach can shut down dispatch for days. Recovery costs dwarf prevention costs. Public trust erodes fast and returns slowly.

This chapter makes one point clear. If cybersecurity and incident auditing are not governed, funded, and enforced as part of the public safety communications system, failure is not a question of if. It is a question of when.

Chapter 9 – Records, Dispatch, and Privacy Controls

Why Records Matter to Safety

Dispatch is not just voices on a radio. It is information moving fast under stress. Addresses, call notes, unit status, medical flags, prior incidents, and warnings all shape what responders do next. If that information is wrong, late, or missing, people get hurt.

Records systems sit at the center of this flow. They link calls, dispatch decisions, radio traffic, and reports. When they work, responders have context. When they fail, dispatch operates blind.

Vermont has treated records systems as back-office tools. They are not. They are safety systems. Governing them poorly creates risk that no amount of radio coverage can fix.

Dispatch and Records Are One System

Dispatch software and records management software are often treated as separate purchases. In practice, they function as one system.

A dispatcher answers a call. The system pulls prior incidents, locations, and warnings. Units are assigned. Notes are logged. After the call, reports flow back into the same system.

When dispatch and records are misaligned, work slows. When data fields do not match, information drops. When access rules differ, users create workarounds. Workarounds create errors.

Governance must treat dispatch and records as a single operational system, not as separate line items.

Fragmentation Creates Blind Spots

Records systems in Vermont vary widely by town and region. Some are modern. Some are outdated. Some are shared. Some are isolated.

Dispatch centers often serve towns that use different records systems. Dispatchers juggle screens or rely on memory. Data sharing across a region becomes unreliable.

During mutual aid events, critical information may not be visible because it lives in another system with no bridge. This is not just a technology problem. It is a governance failure.

Privacy Is Not the Opposite of Access

Privacy concerns are real. Records contain sensitive information: medical notes, domestic violence history, juvenile data.

Privacy is often used as a reason to avoid shared systems. That is a mistake.

Well-designed systems protect data by design. They control who can see what, when, and why. They log access. They allow sharing where authorized and block it where not.

Avoiding shared systems does not protect privacy. It pushes data into email, text messages, and handwritten notes. Those are harder to control and easier to misuse.

Access Rules Must Match Actual Situations

Dispatchers need broad access during active incidents. Investigators may need deeper access later. Supervisors need audit visibility. Not everyone needs everything all the time.

Governance must define these rules clearly. Leaving access decisions to local habit or vendor defaults creates uneven practice and risk.

For example, if one town allows broad access and another locks records tightly, a regional dispatcher faces conflicting rules. Errors follow.

Clear, consistent access standards protect both safety and privacy.

Audit Trails Are Non-Negotiable

Every access to a record should be logged. Who looked. When. Why.

Audit trails protect the public and the dispatcher. Without them, misuse goes undetected. False accusations cannot be resolved. Trust erodes.

Audit capability is not optional. Systems that cannot provide it should not be used for public safety.

Data Retention Has Real Consequences

How long records are kept matters. Too short, and patterns are lost. Too long, and privacy risk grows.

Retention rules should not vary town by town without reason. They should reflect legal requirements, operational needs, and storage costs.

Governance must set and enforce clear retention standards. Otherwise, systems drift toward convenience, not safety.

Integration Raises Cyber Risk

As dispatch and records connect to radios, mobile devices, and broadband, opportunities for attack multiply.

A compromised records system can disrupt dispatch. A stolen login can expose sensitive data across a region.

Security controls discussed elsewhere apply directly here. Strong authentication, segmented access, and monitoring are essential.

Records systems often lag in security because they are treated as administrative. That view is outdated and dangerous.

Funding Decisions Shape Behavior

Records systems cost money to buy, maintain, secure, and upgrade. Grants often cover purchase but not long-term operation.

When funding ignores operating cost, systems age quickly. Updates are delayed. Security patches are skipped. Staff improvise.

Governance must require funding plans that include full lifecycle costs. If a system cannot be sustained, it should not be deployed without restructuring or support.

The Role of the State

The State must set minimum standards for records and dispatch systems: data fields, access rules, audit requirements, security controls, and retention periods.

The State should not pick a single vendor. It should require interoperability and compliance. Systems that cannot meet standards should not be funded.

The State must also ensure that privacy law is applied consistently. Confusion breeds over-restriction, which harms safety.

The Role of Regions

Regions should operate shared records systems where dispatch is shared. This reduces duplication, improves data quality, and supports failover.

Regional governance must enforce common rules. Town-by-town exceptions undermine the whole system.

A Real-World Example

A dispatcher receives a call about a disturbance at an address served by multiple towns. One town's records show a history of violence. Another town's system does not share that data.

The dispatcher assigns units without full context. Responders arrive unprepared.

That is not a privacy success. It is a safety failure.

Why This Cannot Be Left to Vendors

Vendors sell features. They do not decide policy.

If governance does not define access, retention, and audit rules, vendor defaults will. Those defaults reflect general markets, not Vermont law or regional practice.

Clear rules protect vendors as well. They know what to build and what to enforce.

The Cost of Getting This Wrong

Poor records and dispatch integration slows response, increases error, and exposes the State to legal risk. It erodes public trust when data is mishandled.

Fixing these problems later costs more than building them right the first time.

This chapter makes one point clear. Records, dispatch, and privacy controls are not side issues. They are core public safety infrastructure. If they are not governed, funded, and enforced as such, the system will fail quietly until it fails publicly.

CAD Comes Later, Not First

Modern computer-aided dispatch systems add powerful capabilities: real-time mapping, unit location, resource tracking, and incident timelines. In mature systems, CAD improves coordination, accountability, and after-action review.

Those benefits depend on foundations Vermont does not yet have statewide. CAD relies on reliable radio coverage, interoperable dispatch protocols, consistent GIS data, adequate staffing, engineered failover, and clear data governance.

Without those prerequisites, CAD becomes an expensive overlay on fragmented systems. Complexity rises. Training burdens grow. Value falls.

This report does not reject CAD. It places CAD in sequence—as a capstone investment after governance is established, coverage gaps are addressed, failover is engineered, and data standards and privacy controls are enforced.

Proceeding in that order reduces risk, protects public funds, and gives CAD a real chance to deliver its promised value.

Chapter 10 – Pilot Design and Replication

Why Pilots Fail So Often

Vermont has used pilot projects for years. Some worked. Many did not. The problem is rarely effort. It is design.

Pilots are often launched to show progress rather than to answer hard questions. They test equipment without testing governance. They spend grant money without proving long-term cost. They generate anecdotes instead of evidence.

This chapter explains what a pilot must prove to be worth funding, why prior pilots fell short, and why replication fails when pilots are treated as demonstrations instead of tests.

What a Pilot Is Supposed to Prove

A real pilot exists to reduce uncertainty before the State commits at scale.

A valid pilot must show whether governance works under stress. Who decides. Who pays. Who steps in when something breaks.

It must show whether technology performs where responders actually work, not just along highways or near towers.

It must show whether staffing models hold during nights, weekends, storms, and vacancies.

It must show whether operating costs are affordable after grants expire.

If a pilot does not answer these questions, it is not a pilot. It is a preview.

Technology-Only Pilots Mislead

Many pilots focus on gear: new radios, new software, new broadband access.

That is the easy part.

A radio that works during a demo may fail during a storm. Software that works with vendor support may stall when staff are short. Broadband that works on a test route may fail in basements and valleys.

More importantly, technology-only pilots avoid the hardest issue: authority. If no one is forced to make binding decisions during the pilot, nothing real is being tested.

Governance Must Be Tested First

A pilot must force governance into the open.

Who has authority to set rules during the pilot? Who can require participation? Who resolves disputes? Who shuts the pilot down if it fails?

If these questions are left vague, the pilot will appear smooth because no one is allowed to say no.

A useful pilot creates friction on purpose. That friction reveals whether the governance model can actually function.

Funding Sequence Matters

Pilots often appear cheap because grants cover startup costs. That hides the real price.

A proper pilot must track full costs: staffing, maintenance, licensing, connectivity, security, training, and replacement.

If a pilot cannot show how it will be paid for in year five, it cannot be replicated responsibly.

Funding must also be staged. Early money should pay for analysis and setup. Later money should only flow if prerequisites are met. When all money flows up front, learning stops.

Replication Is Where Most Damage Happens

Pilots rarely fail outright. Replication is where mistakes multiply.

A pilot that works in one region may fail in another because terrain differs, staffing differs, or governance differs. Treating a pilot as a template instead of a test spreads those failures statewide.

Replication must require proof that conditions match. If they do not, the model must change. One size does not fit all.

The Danger of Pilots Becoming Commitments

Once a pilot is branded a success, it becomes politically hard to stop. Jobs depend on it. Vendors are invested. Towns adapt around it.

At that point, the pilot has become a commitment without legislative approval.

That reverses the purpose of a pilot. Pilots should preserve legislative choice, not preempt it.

Legal Authority Cannot Be Assumed

Pilots often operate in gray areas: temporary agreements, informal access, workarounds tolerated because the project is “just a pilot.”

Those shortcuts become permanent by habit.

A pilot must operate under the same legal authority required at scale. If the law does not allow it, the pilot should not either. Otherwise, replication forces rule-making under pressure.

Testing legality early avoids crises later.

Technical Dependencies Must Be Exposed

Pilots must surface dependencies, not hide them.

Does dispatch rely on a single fiber route? Does radio coverage depend on one tower? Does records access depend on vendor-hosted servers? Does security rely on one administrator?

If a pilot only works because someone is constantly watching it, it is not resilient. Replication will remove that attention.

Weak points must be known before expansion.

A Concrete Failure Pattern

Consider a pilot that consolidates dispatch for several towns.

During the pilot, the host center has extra staff. Vendor technicians are on call. Backup links are installed temporarily.

Everything works.

After replication, staff return to normal levels. Vendor support costs extra. Temporary links are removed. Failover is untested.

The system fails under load. The pilot did not lie. It simply did not test reality.

The Role of the State

The State must define what a valid pilot looks like. It must require governance testing, full cost accounting, legal compliance, and stress testing.

The State must also be willing to stop a pilot that fails. Calling something a pilot means failure is an option. If failure is politically unacceptable, the project is not a pilot.

The Role of Regions

Regions should propose pilots because they know local conditions. They must also accept that pilots may expose uncomfortable truths about cost, staffing, or authority.

A pilot that only shows success is suspect. A pilot that reveals limits is valuable.

Replication should only occur when regions can show that conditions match or that differences have been addressed.

Why This Chapter Matters

Pilots shape the future more than statutes. They create facts on the ground.

If pilots are poorly designed, they lock the State into fragile systems. If they are designed well, they protect the Legislature from costly mistakes.

This chapter makes one point clear. Pilots are not proof of readiness. They are tests of it. If Vermont treats pilots as demonstrations instead of discipline, replication will repeat every failure the pilots were supposed to prevent.

Chapter 11 – Staffing, Co-Location, and Transition

Why Staffing IS the System

Technology does not answer 911 calls. People do.

Radios, software, and networks fail quietly if there are not enough trained staff to operate them under pressure. Every reform discussed elsewhere collapses if staffing is treated as an afterthought.

Vermont's staffing problem is not just shortage. It is mismatch. Dispatch centers are expected to do more with fewer people, more technology, and more legal exposure, while reforms assume smooth transitions that ignore fatigue, turnover, and training limits.

This chapter explains why staffing must drive design, why co-location is often misunderstood, and why transition planning fails when it is rushed or underfunded.

Dispatch Work Is Not Interchangeable

Dispatch is skilled work. It requires local knowledge, rapid judgment, and emotional control. A trained dispatcher cannot be replaced quickly.

Certification, background checks, and on-the-job learning take time. When staffing plans assume quick hiring or easy transfers, they fail. Burnout rises. Errors increase. Attrition accelerates.

A system that cannot staff itself reliably is not resilient, no matter how modern the equipment.

Regional Models Change the Job

Regional dispatch changes the nature of dispatch work. Call volume increases. Jurisdictions multiply. Policies differ. Stress rises.

That change requires different staffing ratios, different supervision, and different training. Assuming that a regional center can operate with the same staffing model as a small local center is a mistake.

When staffing models do not adjust, the burden shifts to overtime. Overtime is not a plan. It is a warning sign.

Co-Location Is Not a Shortcut

Co-location is often sold as efficiency: put multiple functions in one building, share staff, share space.

Sometimes this works. Often it does not.

Co-locating dispatch with other operations can create noise, distraction, and divided attention. Co-locating regional functions can concentrate risk if power, connectivity, or access fails.

Co-location should be a choice made after risk analysis, not a default driven by real estate or convenience.

A Concrete Example

Consider a regional dispatch center housed in a single building with shared fiber and power. Staffing is lean. Overnight shifts run with minimum coverage.

A winter storm knocks out power and fiber. Backup systems hold for a time. Staff are stretched thin handling calls and managing outages.

If there is no alternate staffed location, service degrades fast. Co-location saved money until it did not.

Failover without staff is fiction.

Training Is a Continuous Cost

Training does not end at hire. New systems require retraining. Policy changes require refreshers. Turnover requires constant onboarding.

Training costs time and money. If budgets only cover positions and not training, skills decay.

Governance must treat training as a standing operational cost. Skipping it to balance a budget creates hidden risk that surfaces later as error or liability.

Transition Is Where Most Harm Occurs

Most failures happen during transitions, not steady state.

When centers merge, systems change, or staff move, normal safeguards weaken. People rely on habit. Temporary rules become permanent. Documentation lags reality.

Transitions require extra staffing, not less. They require overlap periods, not abrupt cutovers. They require patience.

Rushing transition to meet a funding deadline or political promise is reckless.

Legal and Labor Realities Matter

Dispatch staff are governed by labor agreements, certification rules, and employment law. Transitions that ignore these realities fail.

Forcing staff to relocate without adequate notice or compensation drives resignations. Changing job descriptions without retraining exposes liability.

Governance must plan transitions in consultation with labor and regulators. Surprise is the enemy of stability.

Funding Must Match Reality

Staffing is the largest ongoing cost in dispatch. Capital funding does not solve operating gaps.

If regionalization or consolidation increases staffing needs, funding must increase as well. Promising savings through consolidation without proving staffing impacts is misleading.

Stable staffing requires stable revenue. One-time grants do not provide that.

The Role of the State

The State must recognize staffing as core infrastructure. It must ensure that funding models support adequate staffing levels, training, and transition periods.

The State should not mandate structural change without providing resources to manage the human impact. Doing so invites failure and resentment.

The Role of Regions

Regions must be honest about staffing needs and limits. If a region cannot staff a model safely, it should not adopt it.

Regional governance must also protect staff during transitions. Experience is an asset. Losing it through avoidable attrition weakens the system for years.

Why This Chapter Matters

Technology upgrades attract attention. Staffing determines outcomes.

A system with perfect coverage and poor staffing will fail. A system with modest technology and strong staffing can adapt.

This chapter makes one point clear. Staffing, co-location, and transition are not operational details. They are the system. If Vermont plans reform without putting people first, the system will break at the moment it is needed most.

Chapter 12 – Sequencing, Risk, and Political Constraints

Why Order Matters More Than Speed

Public safety communications reform fails when actions happen out of order. Vermont's recent history shows this clearly. Funding moves before authority is settled. Technology decisions are made before staffing is secured. Pilots launch before governance is real.

Speed looks like progress. In reality, it compounds risk.

This chapter explains why sequencing is the central discipline of reform, how risk multiplies when steps are skipped, and how political pressure distorts decision-making unless it is openly constrained.

Sequencing Is a Governance Choice

Sequencing is not a technical detail. It is a decision about what must be true before the next step is allowed.

A regional dispatch center cannot operate safely unless authority is clear, staffing is adequate, funding is stable, and legal rules are settled. If any of those are unresolved, moving forward creates hidden risk.

Good governance enforces order. Weak governance allows exceptions. Exceptions become precedent.

The Cost of Skipping Steps

Skipping steps does not save time. It shifts cost and risk forward.

When funding is committed before governance is clear, money locks in bad structure. When technology is purchased before staffing plans are real, systems sit unused or overstressed. When pilots run before legal authority is settled, workarounds harden into practice.

Each shortcut narrows future choices. By the time problems surface, reversal is politically painful and financially expensive.

Risk Is Cumulative, Not Isolated

Risks do not stand alone. They stack.

A staffing shortage makes technology failures harder to manage. Weak cybersecurity makes records systems fragile. Fragmented authority slows response during outages.

When multiple risks align, failure becomes likely.

Good sequencing reduces compounding risk by resolving foundational issues first. Bad sequencing does the opposite.

Political Pressure Is Predictable

Elected officials face pressure to show action. Grants come with deadlines. Vendors promise quick wins. Crises demand visible response.

None of this is malicious. It is normal.

The problem arises when political urgency overrides structural readiness. Declaring success early does not make systems safer. It delays accountability.

A system built to meet a press-release deadline will eventually meet reality.

Irreversible vs. Reversible Decisions

Some decisions can be undone easily. Others cannot.

Hiring temporary staff is reversible. Selling a building is not. Piloting software is reversible. Signing a long-term statewide contract is not.

Sequencing must protect reversibility early and defer irreversible commitments until prerequisites are met. When irreversible decisions come too soon, learning stops.

Vermont has too often reversed this logic.

Funding Creates Momentum

Money drives behavior. Once funds are allocated, pressure builds to spend them, even if conditions are not ready.

This is why funding must be sequenced behind governance and standards. If money flows first, discipline erodes. If money flows last, it reinforces compliance.

Funding without guardrails is not support. It is leverage in the wrong direction.

Legal Authority Cannot Be Assumed Into Place

Legal authority does not appear because a project exists. It must be established first.

If regional governance powers are unclear, acting as if they exist creates risk. If privacy rules are unsettled, sharing data anyway creates exposure. If labor authority is incomplete, staffing plans will break.

Sequencing law behind action invites challenge and backlash. Settling authority first protects both the system and the Legislature.

Technical Dependencies Are Not Optional

Public safety communications depend on land mobile radio for voice, broadband for data, fiber for backhaul, and software for dispatch and records. Each has limits.

Sequencing must respect those limits. Broadband cannot replace radio where coverage is weak. Fiber cannot be assumed redundant without mapped routes. Software cannot compensate for human overload.

Ignoring these dependencies produces brittle systems that look modern but fail under stress.

A Concrete Failure Pattern

Consider a region that receives funding to consolidate dispatch quickly.

Governance agreements are incomplete. Staffing plans assume transfers that do not occur. Technology is installed anyway.

Dispatchers work overtime. Systems strain. Outages occur. Towns lose confidence. Political support erodes.

The failure is blamed on resistance or bad luck. In reality, the sequence was wrong from the start.

Political Constraints Must Be Named

Politics does not disappear because a report is written. It must be acknowledged and constrained.

That means admitting when a deadline is political rather than operational. It means setting conditions that cannot be waived quietly. It means accepting slower progress over fragile success.

Legislators need cover to say no. Clear sequencing provides that cover.

The Role of the Legislature

The Legislature's job is not to manage projects. It is to set conditions.

By defining required order, the Legislature protects itself from pressure to fund incomplete systems. It also protects local governments from being rushed into commitments they cannot sustain.

Clear sequencing is a legislative safeguard.

The Role of the Executive

Executive agencies execute within constraints.

When sequencing is clear, agencies can say no to premature demands. When it is vague, agencies absorb pressure and pass risk downward.

Clear order strengthens executive discipline rather than weakening it.

The Role of Regions and Towns

Local governments feel the impact of poor sequencing first. Staffing stress, service degradation, and public complaints land locally.

Regions and towns need explicit permission to slow down when prerequisites are missing. Sequencing rules provide that permission.

Why This Chapter Closes the Report

Everything discussed in earlier chapters depends on order.

Governance before funding. Staffing before consolidation. Authority before technology. Security before integration.

This chapter makes one final point. Reform fails not because Vermont lacks ideas or effort. It fails when impatience overrides sequence.

If Vermont wants a public safety communications system that works when it matters, it must accept a simple discipline: do the right things in the right order, even when politics pushes otherwise.

Appendix A:

Predictable Public Safety Failures — Vermont-Scale Narratives

This appendix presents composite, Vermont-scale narratives grounded in documented conditions and known failure modes. They are not accusations and do not identify individuals or agencies. Each narrative illustrates how ordinary events can cascade into preventable risk when systems rely on informal workarounds rather than engineered resilience, unified standards, and accountable governance as proposed in this report.

1. The Call That Can’t Be Made

A winter outage takes down commercial power across a rural area. Copper landlines have been retired in favor of fiber-based voice service that depends on customer-side power. After a short battery window, the terminal goes dark. Cellular coverage is unavailable. No call for help can be made, and no incident is logged.

2. The Ambulance Decision

An EMS crew loses LTE connectivity while transporting a borderline patient. Telemetry and coordination tools drop offline, forcing decisions with incomplete information. The outcome is acceptable, but the risk created by assumed connectivity remains.

3. The Quiet Shift

A dispatch delay occurs due to ordinary human factors. Without engineered detection or escalation, the system relies on individual vigilance rather than structural safeguards.

4. Inside the Building

Responders lose radio and LTE connectivity inside a dense, retrofitted building lacking in-building enhancement systems. Command decisions proceed with partial visibility.

These narratives illustrate predictable conditions addressed by the governance, standards, and resilience measures proposed in this report.

Appendix B:

Documented Warnings and Rejected Public Safety Resilience Concerns

This appendix provides a curated extract of documented public comments and agency responses demonstrating that concerns regarding public safety communications resilience and redundancy were raised in advance and formally declined. The purpose is to establish foreseeability in support of this report.

A. Public Safety Systems Treated as Out of Scope

Comments argued that LMR, dispatch, and public safety backhaul constitute telecommunications systems essential to emergency response. Responses declined to incorporate these systems into statewide planning.

B. Dispatch Failover and Backup Power

Specific concerns regarding dispatch survivability, backup power auditing, and inter-regional failover were acknowledged but not adopted due to scope limitations.

C. Cellular Coverage and Emergency Calling

Comments documented persistent cellular gaps and warned that copper retirement would reduce emergency calling resilience. Responses relied on existing coverage models without adopting equivalent resilience requirements.

These records demonstrate that the failure modes addressed in this report were foreseeable.

Appendix C:

Failed Oversight and Jurisdictional Evasion

This appendix documents formal efforts to obtain regulatory oversight of public safety communications reliability and the jurisdictional arguments that prevented resolution, creating a governance vacuum addressed by this report.

A. Petitions for Oversight

After planning processes failed to resolve resilience concerns, petitions sought review by the Public Utility Commission.

B. Jurisdictional Objections

The 911 Board asserted exclusive authority over 911 operations, precluding PUC review of system reliability.

C. Resulting Vacuum

No agency retained clear authority to mandate resilience standards, testing, or accountability.

This report proposes explicit authority and unified governance to close this gap.

Appendix D:

Glossary of Public Safety Communications Terms

This glossary supports readers without technical backgrounds and is provided for reference throughout this report.

- **PSAP** (Public Safety Answering Point): The initial, 24/7 call center answering 9-1-1 calls, often called a 911 Communications Center.
- **Dispatch/Dispatch Center** The location or process where emergency responders (police, fire, EMS) are assigned and coordinated to incidents.
- **Primary PSAP** Receives 9-1-1 calls directly from the phone network.
- **Secondary PSAP** Receives 9-1-1 calls transferred from a Primary PSAP (e.g., for specialized services like fire or EMS)**.**
- **ECC (Emergency Communications Center)** A general term for centers that handle 9-1-1 call-taking, dispatching, or both.
- **CAD** (Computer-Aided Dispatch): A computer system used to manage calls for service, prioritize them, and dispatch resources.
- **ALI** (Automatic Location Identification): A feature that displays the caller's address or location on the screen.
- **ANI** (Automatic Number Identification): A feature that displays the caller's phone number.
- **Telecommunicator** The certified professional who answers emergency calls and/or dispatches units.
- **Next Generation 9-1-1 (NG911)** An IP-based system allowing digital information (text, video, data) to flow from the public to emergency responders.
- **Consolidated PSAP** Multiple agencies working together in one center for improved efficiency.
- **SOP (Standard Operating Procedures)** Written guidelines dictating how emergencies are handled.
- **Status Code** Alphanumeric codes indicating the status of a field unit (e.g., en route, on scene).
- **Backhaul** Network connections carrying traffic from field sites to core networks.
- **Failover** The ability to transfer operations to a backup system when the primary fails.
- **LMR** Land Mobile Radio used for mission-critical public safety voice communications.
- **LTE** Cellular broadband technology used for voice and data services.
- **UPS** Uninterruptible Power Supply providing short-term backup power.

Appendix E:

Relevant Statutory Language
(Act 78 and Act 87, Consolidated for Readability)

This appendix reproduces the relevant statutory language governing the Public Safety Communications Task Force and the congressionally directed public safety communications funds. For readability, the text reflects the operative language as enacted, consolidated from the original Act 78 provisions and the subsequent Act 87 Budget Adjustment Act amendments. No substantive changes have been made.

Act 78

Sec. C.114 PUBLIC SAFETY COMMUNICATIONS SYSTEM; DISPATCH; INVENTORY; DESIGN

(a) The General Assembly finds that protecting public safety and welfare is an essential function of State government and it is in the public interest to establish a statewide reliable, secure, and interoperable public safety communications system, comprising integrated 911 call-taking and regional dispatch systems, and to ensure that the system is equitably and sustainably financed and universally accessible by all persons throughout the State.

(b) It is not the intent of the General Assembly to establish a public safety communications system that disrupts or in any way jeopardizes the exceptional dispatch services currently in place or the existing 911 system, but rather to support, enhance, strengthen, and build upon those efforts and initiatives.

(c) The transition to a public safety communications system as specified in subsection (a) of this section shall be overseen and managed by the temporary Public Safety Communications Task Force established in subsection (d) of this section.

(d)

(1) There is established a **Public Safety Communications Task Force** to oversee and manage all phases of the development, design, and implementation of a statewide public safety communications system as required by this section.

(2) The Task Force shall consist of seven members as follows:

(A) the **Executive Director of the Enhanced 911** Board, who shall serve as Co-Chair;

(B) the **Commissioner of Public Safety** or designee, who shall serve as Co-Chair;

(C) one **municipal official** appointed by the Executive Director of the Vermont League of Cities and Towns;

(D) one representative from a public safety answering point overseen by a municipal police department **appointed by the Vermont Association of Chiefs of Police**;

(E) one **emergency medical technician or paramedic** appointed by the Vermont State Ambulance Association;

(F) one firefighter appointed by the **Vermont State Firefighters' Association**; and

(G) the **Chair of the Regional Dispatch Working Group** established by the General Assembly in Act 185 of 2022.

(3) At its initial organizational meeting the Task Force shall elect from among its members a vice chair. Meetings may be held at the call of a Co-Chair or at the request of two members. A majority of sitting members shall constitute a quorum, and action taken by the Task Force may be authorized by a majority of the members present and voting. Except for those members regularly employed by the State, members are entitled to a per diem in the amount of $150 for each day spent in the performance of their duties. All members, including members otherwise regularly employed by the State, shall receive their actual and necessary expenses when away from home or office upon their official duties pursuant to this section. A vacancy shall be filled by the respective appointing authority. If the Chair of the Regional Dispatch Working Group declines to participate as a member of the Task Force, the Task Force shall appoint one member who shall have expertise relevant to the purposes of this section.

(4) The Task Force is authorized to retain a project manager and one or more additional consultants with relevant expertise in public safety communications technology, design, and financing to assist with the requirements of this section.

(5) The Department of Public Safety shall provide the

Task Force with administrative services and support.

(6)

(A) The Task Force, in consultation with the Secretary of Administration, shall develop procedures and best practices for State agency cooperation and coordination on matters of overlapping jurisdiction. The primary purpose of this subdivision is to ensure the Task Force has access to expertise and data related to its mission, including expertise within and data maintained by the Department of Public Service, the Agency of Digital Services, the Division of Emergency Preparedness, Response and Injury within the Department of Health, the Department of Taxes, the Agency of Transportation, the Enhanced 911 Board, and the Department of Public Safety.

(B) Nothing in this subdivision shall be construed to waive any privilege or protection otherwise afforded information by law due solely to the fact that the information is shared with the Task Force pursuant to this subdivision.

(7) All meetings of the Task Force shall be open to the public and conducted in accordance with the Vermont Open Meeting Law. All records of the Task Force are subject to the Vermont Public Records Act.

(8) The Task Force shall cease to exist when a State entity authorized by legislative enactment to permanently oversee and manage the public safety communications system becomes operational.

(e) The establishment of a statewide public safety communications system shall occur in essentially three phases, which include data collection and analysis, design, and implementation. Certain aspects of each phase may occur simultaneously as deemed appropriate by the Task Force.

(1) Data collection and analysis. On or before September 15, 2024, the Task Force shall conduct a complete inventory and assessment of all aspects of dispatch service currently provided in Vermont and, to the extent

possible, dispatch service currently provided outside Vermont for response agencies located in Vermont, which shall include:

(A) an inventory of all existing dispatch infrastructure and equipment, including facilities, hardware, software, applications, and land mobile radio systems, referring to and incorporating any existing relevant data collected by a State or municipal entity;

(B) the number of full-time and part-time personnel currently performing dispatch service, taking into account personnel who have other responsibilities in addition to providing dispatch service;

(C) the current total spending on dispatch service in Vermont that includes and itemizes for each municipality and dispatch center all federal, State, and municipal appropriations and fees, every contract for dispatch or first responder service, and projected budgets;

(D) identification of the communications dead zones in the State, meaning those areas that lack the infrastructure to support public safety land-mobile-radio communications or cellular voice and data service, or both, and taking into consideration all cell towers, including those that are part of the FirstNet statewide public safety radio access network; cellular mapping efforts conducted by the Department of Public Service; and any existing, relevant mapping data collected by a dispatch center or other entity;

(E) with the assistance of the Vermont League of Cities and Towns, a needs assessment to determine where and to what extent there are gaps in dispatch service or significant challenges to the delivery of dispatch service and to identify those municipalities that are likely to be most affected by either the curtailment of dispatch service from the two State-run public safety answering points or from a new financing mechanism for the continuation

of such service;

(F) an assessment of the service provided by each dispatch center and identification of particular challenges or vulnerabilities, if any, including with regard to workforce, failover procedures, communications technology, costs, and governance; and

(G) collection and assessment of any other information the Task Force deems relevant.

(2) Design. On or before January 15, 2024, the Task Force shall develop findings and recommendations related to draft elements of a preliminary design for a public safety communications system, including identification of a proposed implementation timeline and any additional data and resources needed to develop a final design on or before December 15, 2024. The final design shall include:

(A) technical and operational standards and protocols that ensure an interoperable and resilient system that incorporates computer-aided dispatch systems and land mobile radios;

(B) technology life-cycle standards to ensure system and database upgrades are timely, sufficiently financed, and properly managed;

(C) system and database security and cybersecurity standards;

(D) continuity of operations standards and best practices that encompass failover procedures and other system redundancies to ensure the continuous performance of mission-critical operations;

(E) workforce training standards and other staffing best practices that support the retention and well-being of dispatch personnel;

(F) a resource allocation plan that ensures dispatch service is available in all regions of the State, including the establishment of new dispatch centers

or expanded capacity and capability of existing dispatch centers, if deemed appropriate by the Task Force;

(G) a process for annually reviewing the budgets of dispatch centers;

(H) a recommended governance model to ensure effective State and regional oversight, management, and continuous improvement of the system, including identification of staffing or operational needs to support such oversight and management of the system;

(I) cost estimates for implementing the system in Vermont, including operational and capital costs;

(J) options for sustainably and equitably structuring the financing of the public safety communications system, taking into consideration:

(i) existing budgets for regional and local dispatch;

(ii) the population, grand list, and call volume of each municipality;

(iii) existing and potential State funding streams;

(iv) available federal funding opportunities for public safety agencies and emergency communications systems, including equipment, network infrastructure, and services;

(v) financing models adopted in other jurisdictions for public safety communications systems; and

(vi) any other standards or procedures deemed necessary or appropriate by the Task Force.

(f)

(1) If the Task Force determines that sufficient minimum technical and operational standards have been developed

to warrant the funding of one or more pilot projects, the Task Force may submit for approval a pilot project plan to the Joint Fiscal Committee in calendar year 2023.

(2) Pilot projects eligible for funding under this subsection may include new regional dispatch centers or expanded capacity at existing regional dispatch centers, provided the Task Force determines the pilot demonstrates project readiness and is otherwise consistent with the standards and purposes of this section.

(3) In evaluating proposed pilot projects, the Task Force shall give a high priority to projects in geographical areas of the State that presently face significant challenges with respect to reliably providing dispatch service.

(4) The pilot project plan shall include a description of each proposed project, the resources needed, and an explanation of how the project will align with, inform, and further the development of a statewide public safety communications system and ensure transparency and accountability particularly with respect to the expenditure of State funds pursuant to this subsection.

(5) The Joint Fiscal Committee is authorized to approve up to $4,500,000.00 in total for pilot projects authorized by this subsection.

(g) On or before January 15, 2024, the Task Force shall submit a progress report on the data collection and analysis required by subdivision (e)(1) of this section, the findings and recommendations required by subdivision (e)(2) of this section, and a description and status report of any pilot projects funded pursuant to subsection (f) of this section in a written report to the Senate Committees on Government Operations and on Finance and the House Committees on Government Operations and Military Affairs, on Ways and Means, and on Environment and Energy. On or before December 15, 2024, the Task Force shall submit to the same legislative committees a written report containing its final design plan as required by subdivision (e)(2) of this section.

Sec. C.115 2022 Acts and Resolves No. 185, Sec. B.1100 is amended to read:

Sec. B.1100 FISCAL YEAR 2023 ONE-TIME GENERAL FUND APPROPRIATIONS

* * *

(b) $11,000,000 is appropriated from the General Fund to the Department of Public Safety for regional dispatch funding. The funds are subject to the following conditions:

(1) ~~$4,500,000 shall be held in reserve until the report required by Sec. E.209.1 of this act is submitted and further approval to expend the funds is granted by the General Assembly~~ Up to $1,000,000 shall be available for the retention of technical experts to assist the Task Force with the analysis and planning required by Sec. C.112 of this act and to fund the administrative expenses incurred by the Public Safety Communications Task Force. If the Task Force determines in calendar year 2023 that additional funding is necessary to achieve its purposes, it may submit a request to the Joint Fiscal Committee. The Joint Fiscal Committee is authorized to approve up to an additional $1,000,000.

(2) ~~$6,500,000 to provide grants to regional dispatch facilities upon approval of the Joint Fiscal Committee susbsequent to review of a Regional Dispatch Facility grant plan submited by the Commissioner of Public Safety. The plan shall include the extent to which federal funding sources may be available for regional dispatch~~ Up to $4,500,000 shall be available to provide funding for pilot projects pursuant to Sec. C.112(f), of this act.

(3) Any remaining amounts not obligated pursuant to subdivisions (1) and (2) of this subsection (b) shall be held in reserve until approval to expend the funds is authorized by further enactment of the General Assembly.

(4) It is the intent of the General Assembly that the Department of Public Safety seek to draw and deploy the $9,000,000 in Congressionally Directed Spending to support Vermont’s transition to a modernized, regional communications network in a manner that coordinates with and advances the

goals of a statewide public safety communications system. The Commissioner of Public Safety shall consult with the Public Safety Communications Task Force as the federal parameters for expending the funds become available and as the Commissioner develops a plan to expend such funds. In addition, the Commissioner shall update the Joint Fiscal Committee on planned expenditures.

* * *

Sec. C.116 VERMONT UNIVERSAL SERVICE FUND; JOINT FISCAL OFFICE STUDY

On or before January 15, 2024, the Joint Fiscal Office shall analyze options for changing the financing mechanism for the Vermont Universal Service Fund to ensure the long-term sustainability of the programs funded through the Vermont Universal Service Fund, including the Enhanced 911 system. The Joint Fiscal Office may consider and further refine the analysis and recommendations included in the Secretary of Administration’s report related to the funding of Enhanced 911 operations, dated January 15, 2022, and required by 2021 Acts and Resolves No. 74, Sec. E.235.

Act 87, Section 49

* * *

Sec. 49. 2022 Acts and Resolves No. 185, Sec. B.1100, as amended by 2023 Acts and Resolves No. 78, Sec. C.115, is further amended to read:

Sec. B.1100 FISCAL YEAR 2023 ONE-TIME GENERAL FUND APPROPRIATIONS

* * *

(b) $11,000,000 is appropriated from the General Fund to the Department of Public Safety for regional dispatch funding. The funds are subject to the following conditions:

(1) Up to $1,000,000 shall be available for the retention of technical experts to assist the Public Safety Communications Task Force with the analysis and planning required by 2023 Acts and Resolves No. 78, Sec. C.114 and to fund the administrative expenses incurred by the Public Safety Communications Task Force. If the Task Force determines that additional funding is necessary to achieve its purposes, it may submit a request to the Joint Fiscal Committee.

The Joint Fiscal Committee is authorized to approve up to an additional $1,000,000.

(2) Up to $4,500,000 shall be available to provide funding for pilot projects pursuant to 2023 Acts and Resolves No. 78, Sec. C.114(f).

(3) Any remaining amounts not obligated pursuant to subdivisions (1) and (2) of this subsection shall remain unobligated and unexpended until approval to expend the funds is authorized by further enactment of the General Assembly.

(4) In order to extract the greatest value from the limited State and federal dollars currently available for public safety communications modernization, it is the intent of the General Assembly that all such funding is expended in an efficient and complementary manner. To that end, the Commissioner of Public Safety shall seek to draw and deploy the $9,000,000 in Congressionally Directed Spending to support Vermont's transition to a modernized, regional communications network in a manner that coordinates with and advances, to the greatest extent possible, the statewide public safety communications system developed by the Public Safety Communications Task Force. The Commissioner of Public Safety shall promptly inform the Public Safety Communications Task Force as the federal parameters for expending the funds become available and as the Commissioner develops and, if necessary, revises the plan to expend such funds. The Commissioner shall solicit recommendations from the Task Force regarding the plan, including any revisions to the plan, the implementation schedule, and specific expenditures. In addition, the Commissioner shall update the Joint Fiscal Committee on planned expenditures.

* * *

Sec. 50. 2023 Acts and Resolves No. 78, Sec. C.114(f) is amended to read:

(f)(1) If the Task Force determines that sufficient minimum technical and operational standards have been developed to warrant the funding of one or more pilot projects, the Task Force may submit for approval a pilot project plan to the Joint Fiscal Committee.

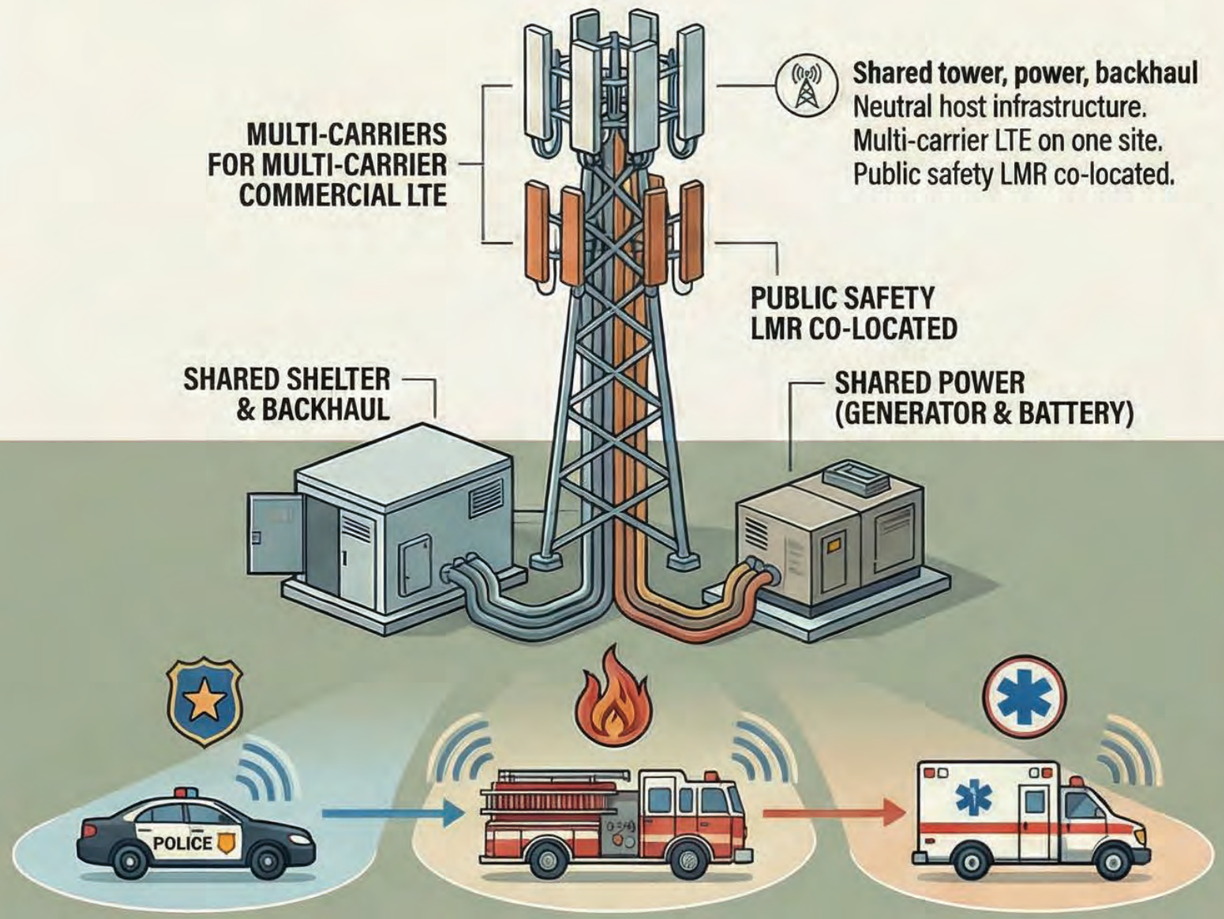
* * *

Appendix F:

Neutral Host Cellular + LMR
vs
Fragmented Tower Competition Clutter

Infrastructure Logic: Shared vs. Fragmented Public Safety Communications

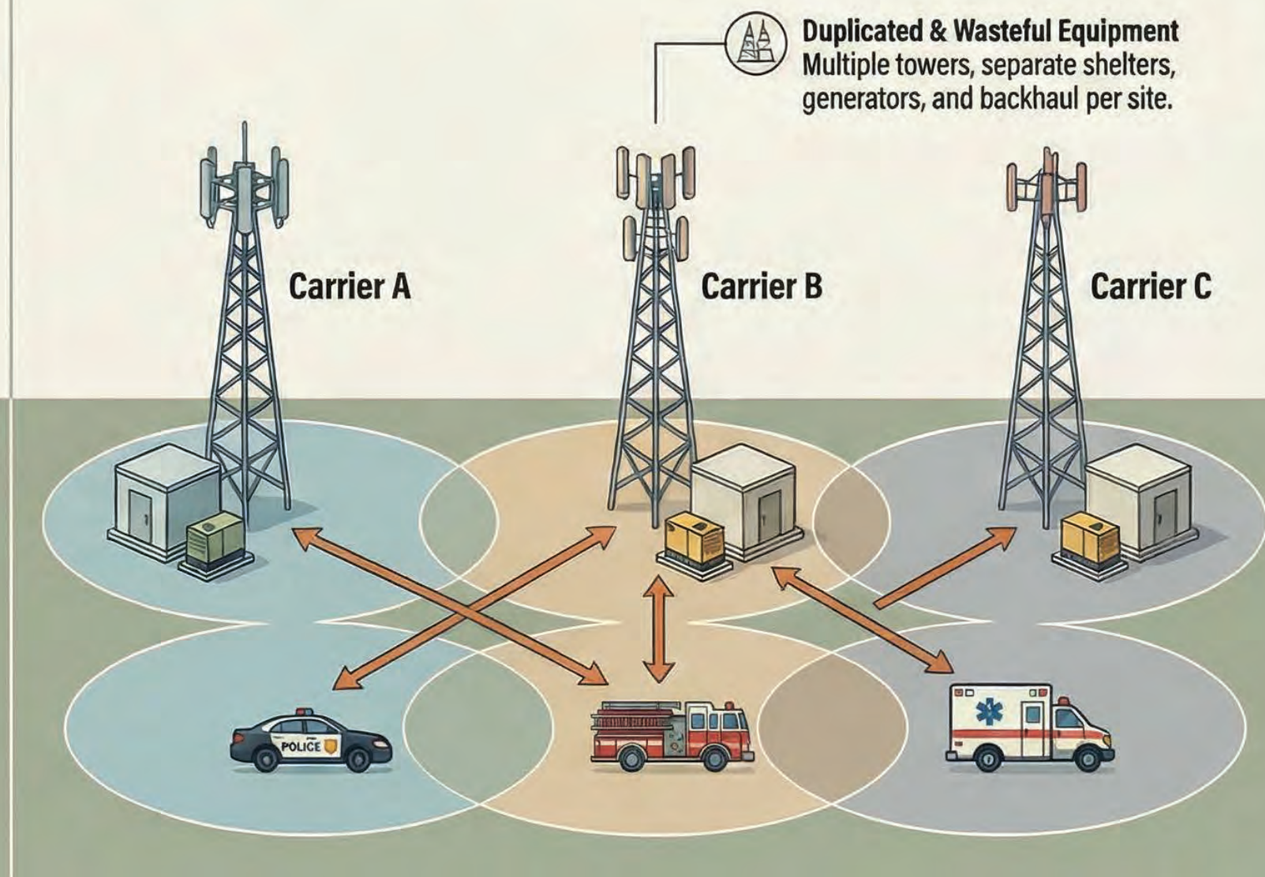
Neutral Host & Co-Location Model
(Shared Infrastructure)



Fewer towers, shared infrastructure, resilient coverage, true multi-carrier fallover for public safety users.

Feature: Total Tower Count	**Neutral Host Model:** Fewer towers; efficient land use
Feature: Power Systems	**Neutral Host Model:** Shared generators and battery backup
Feature: Safety Impact	**Neutral Host Model:** Resilient, multi-carrier failover

Carrier-by-Carrier Buildout
(Fragmented Infrastructure)



More towers, duplicated equipment, persistent dead zones, no guaranteed failover.

Feature: Total Tower Count	**Carrier-by-Carrier Model:** More towers; duplicated footprint
Feature: Power Systems	**Carrier-by-Carrier Model:** Individual, redundant power per site
Feature: Safety Impact	**Carrier-by-Carrier Model:** Brittle systems with coverag