

PUBLIC SAFETY · LAW ENFORCEMENT · SECURE CONNECTIVITY AT CITY SCALE

# A metropolitan police service ran dispersed operations without a network of its own — 24 locations were put on one secure, private citywide wireless network, surveyed to commissioned in four months.

A metropolitan police service's citywide secure network — point-to-point and point-to-multipoint fixed wireless on hardened infrastructure across 24 locations, with guaranteed committed-rate links, centralized communication, and the service's own team trained to run it.

<p><b>CLIENT</b> A metropolitan police service (anonymized)</p>	<p><b>ROLE</b> Project Manager — secure network deployment</p>	<p><b>ENGAGEMENT IN NUMBERS</b> 24 locations commissioned · guaranteed committed-rate (CIR) links · acceptance criteria + bench tests · milestone sign-offs</p>
<p><b>DURATION</b> 4 months · team of four</p>	<p><b>PLATFORM / INFRASTRUCTURE</b> Fixed wireless (WiMAX 802.16d) PtP / PtMP on hardened network infrastructure · network-management suite</p>	<p><b>PROGRAM SCALE</b> A citywide private network giving a police service centralized, secure communication across its operating locations</p>

## 01 The mandate

A metropolitan police service operated across two dozen dispersed locations without a secure network of its own connecting them. Centralized communication — the basic nervous system of coordinated policing — depended on infrastructure the service did not control. The initiative existed to change that: a private, secure, citywide wireless network owned by the service, linking every operating location with guaranteed committed bandwidth.

The deployment had to be done properly and quickly: site surveys across the city, installation, configuration, and commissioning at 24 locations, civil and electrical works subcontracted and supervised, and the service's own team trained on the network-management suite — from plan to commissioned network in four months.

## 02 The delivery context

### A police network is judged on trust, not throughput

For a law-enforcement service, the point of a private network is control: secure links it owns, guaranteed committed rates it can rely on, and management tooling its own people operate. Every design and acceptance decision was framed around dependable, secure communication for operations — not consumer-grade connectivity.

### Twenty-four sites, many trades, one short schedule

Each location carried its own survey, civil, electrical, and installation realities, with third-party contractors doing the physical works and a four-month window over the whole program. The schedule lived or died on disciplined sequencing of surveys, trades, equipment, and commissioning across the city.

## 03 How the engagement was run

### Acceptance defined before deployment

Developed the project management plan with explicit acceptance-test criteria and success measures up front, conducted equipment bench testing before anything was installed on the client's premises, and obtained client sign-off at each milestone — surveys, deployment, testing, commissioning, and training — so 'done' was never in dispute.

### Roles, contractors, and supply chain held to account

Created the responsibility-assignment matrix for client and vendor roles from the RFP's terms of reference, defined team responsibilities through RACI, developed the bill of materials with the channel partner, and subcontracted the civil and electrical works to third parties whose performance was actively monitored.

### Commissioned, then handed to the service's own team

Sequenced site surveys, installation, configuration, and commissioning across all 24 locations on a defined resource calendar, ran weekly status meetings with risk register and issue log live, and trained the service's team on the network-management suite — so the police owned and operated their network from day one.

## 04 Outcome

All 24 locations were surveyed, installed, configured, and commissioned onto one private, secure citywide wireless network in four months by a team of four — with guaranteed committed-rate links, centralized communication established across the service's operating locations, and the service's own staff trained on the network-management suite. Every milestone carried documented client sign-off against acceptance criteria defined before deployment began. Commercial figures are held confidential; the result is a police service that went from depending on infrastructure it did not control to operating a secure network of its own.

DEPLOYED AND COMMISSIONED	SCALE
Operating locations on the private network	<b>24 — surveyed, installed, commissioned</b>
Link types	<b>Point-to-point and point-to-multipoint fixed wireless</b>
Service level	<b>Guaranteed committed information rate per link</b>
Quality gates	<b>Bench tests before install · acceptance criteria · milestone sign-offs</b>
<b>Delivered</b>	<b>4 months · team of four · client team trained on NMS</b>

**OUTCOME POSTURE****24 locations. One private, secure citywide network. Four months, a team of four.**

Secure connectivity delivered as a capability: a police service moved from infrastructure it did not control to a network it owns, operates, and trusts — with acceptance proven at every milestone.

**05 What this demonstrates****Built secure connectivity for a law-enforcement service.**

Put 24 dispersed police locations on one private citywide network with guaranteed committed-rate links and centralized communication.

**OFFERED TODAY AS: SECURE NETWORK DELIVERY****Defined acceptance before deployment.**

Acceptance-test criteria and bench testing set before installation, with documented client sign-off at every milestone from survey to training.

**OFFERED TODAY AS: QUALITY & ACCEPTANCE GOVERNANCE****Managed trades and vendors across a city.**

Subcontracted and supervised civil and electrical works at 24 sites, with a RAM/RACI holding client, vendor, and contractor roles to account.

**OFFERED TODAY AS: CONTRACTOR & VENDOR MANAGEMENT****Delivered fast without skipping the discipline**

Surveys to commissioning in four months with a team of four — on a defined resource calendar, with live risk and issue registers and weekly status governance.

**OFFERED TODAY AS: PROGRAM MANAGEMENT****Handed over an operating capability.**

Trained the service's own team on the network-management suite so the police ran their network from day one.

**OFFERED TODAY AS: CHANGE & TRAINING****SOURCE ARTIFACTS AND DISCLOSURE**

Anonymized for the law-enforcement nature of the engagement: the service, city, vendor products, and commercial figures are withheld. Figures represent counts recorded in engagement documentation held by the practice — the project plan and acceptance criteria, site survey and commissioning records, and milestone sign-offs.

Premium Framework Inc. is an independent IT project, program, and PMO leadership practice — founded 2011 — serving federal government, provincial agencies, public-sector institutions, and large enterprise organizations in regulated, high-stakes environments. The Delivery Track Record series presents named, source-substantiated program engagements.

**Talk to a delivery expert**

[sz@premiumframework.ca](mailto:sz@premiumframework.ca) · +1 613-600-2803 (Mon–Fri, 9–5 ET) · [calendly.com/it\\_delivery\\_management](https://calendly.com/it_delivery_management)

Tailored briefs for specific sectors or program types are available on request. Additional engagements held under confidentiality are available for discussion under NDA.