PREMIUM FRAMEWORK

CASE SUMMARY · DELIVERY TRACK RECORD

PUBLIC SAFETY · LAW ENFORCEMENT · SECURITY-CRITICAL CAPABILITY ESTABLISHMENT

A transit special-constable unit was holding criminal-justice information in spreadsheets and a filing cabinet — it was given a security-cleared, CPIC-compliant dispatch and records capability by joining a province-wide police cooperative, not building one or surrendering its data to another force.

OC Transpo Transit Law's policing-capability establishment — moving investigative information from spreadsheets and a filing cabinet to dispatch, records, interoperability, and nationally compliant access, by joining an existing law-enforcement ecosystem rather than building or buying alone.

CLIENT **City of Ottawa — OC Transpo (Transit Law / Special Constables Unit)**	ROLE **Project Manager — OC Transpo Technology and Control System**	VENDOR / PLATFORM **Provincial law-enforcement cooperative — standard CAD + records platforms (generalized)**
ENGAGEMENT MODEL **Single accountable PM across sourcing, security, requirements, and rollout**	DURATION **2015 · 18-month program**	PROGRAM SCALE **A sworn special-constable unit · segregated criminal-justice network · full unit trained onto the system**

01 The mandate

Transit special constables are designated as police officers for twenty sections of the Criminal Code, yet the sensitive investigative information they collected lived in an Oracle application, spreadsheets, and a filing cabinet — on city servers reachable by staff without police clearance. There was no secure records system, no way to cross-reference findings across incidents, and only a limited ability to run national police checks.

The unit needed a genuine records-management and computer-aided-dispatch capability: one that meets national police-information-centre requirements, sits on a properly secured and segregated network, and can share investigative information with the provincial police and national systems — without the cost and timeline of building it alone.

02 The delivery context

Security was the design driver, not a workstream

This was not a normal IT system, and security was not a stream of work bolted on beside the others — it was the design driver. National police-information-centre connection rules and a national security framework determined the architecture (a network segregated from city IT), the sourcing strategy (who could host and own

the data), the deployment sequence (security stood up before any operational use), and the operating model (enhanced-clearance access, certificate-based authentication, controlled physical access). Security came first and everything else followed from it.

Who owns the data was the decisive question

The unit needed to share investigative information with the provincial police and national systems — but on terms that kept ownership of its own records. Interoperability without ownership would have solved one problem and created a worse one, and that single consideration shaped the entire sourcing decision.

03 How the engagement was run

A third option beyond build and buy: join an existing ecosystem

Most organizations frame a capability like this as build versus buy. A third path was put on the table and chosen: join the province-wide law-enforcement cooperative already used by dozens of agencies — inheriting its proven platforms, standard practices, security framework, and information sharing, with its collective buying power, while retaining ownership of the unit's own records. Status quo and a costly partnership with the municipal police service (which would have owned the data) were both rejected on interoperability, security compliance, and ownership.

Built to criminal-justice security standards first

A law-enforcement network segregated from city IT, enhanced-clearance access, certificate-based authentication, and controlled physical security were stood up to satisfy the national connection-authorization and security framework before the system went into operational use — the order a policing system requires.

Configured for operations and a trained unit

Operational requirements — event types, beat maps, naming conventions, the data-element set — were gathered with the unit and the cooperative's specialists, the platforms were installed, configured, and tested, and a trainer-led program brought the unit's registrar authorities, system trainers, and 60+ constables and staff onto the system.

04 Outcome

The unit crossed a capability gap, not an upgrade. Before: spreadsheets, a filing cabinet, only limited national police checks, and no way to cross-reference incidents. After: real computer-aided dispatch and records, interoperability with the provincial police and national systems, and compliant access on a secured network — investigative information moved from unsecured storage to a nationally compliant criminal-justice environment. It was delivered by joining a province-wide law-enforcement cooperative rather than building alone or surrendering data ownership, with a trainer-led program bringing the unit's registrar authorities, trainers, and constables onto the system. Commercial figures are held confidential.

SOURCING OPTIONS FOR THE CAPABILITY	ASSESSMENT
Keep the status quo — spreadsheets and a filing cabinet	**Rejected — no secure records, no national checks**
Partner with the municipal police service	**Rejected — high cost; that service would own the records**
Join the province-wide law-enforcement cooperative	**Selected — interoperability, security compliance, data retained**
Result	**Compliant capability without building from scratch**

OUTCOME POSTURE

From spreadsheets and a filing cabinet to a nationally compliant criminal-justice capability — by joining an ecosystem, not building or buying alone.

Not a system implementation but the creation of a policing capability: secure records, dispatch, and interoperability stood up to national standards, through a third sourcing path most organizations never consider.

05 What this demonstrates

Criminal-justice capability establishment.

Crossed a capability gap — from spreadsheets and a filing cabinet to dispatch, records, interoperability, and compliant access — building a nationally compliant policing capability where none existed.

OFFERED TODAY AS: CAPABILITY ESTABLISHMENT

Security as the operating requirement.

Moved investigative information from unsecured storage to a nationally compliant criminal-justice environment, with security standards driving the architecture, sourcing, sequence, and operating model.

OFFERED TODAY AS: SECURE SYSTEMS DELIVERY

Ecosystem sourcing — beyond build vs. buy.

Introduced a third option beyond build or buy — joining an existing law-enforcement ecosystem — and chose it on interoperability, security compliance, and data ownership.

OFFERED TODAY AS: SOURCING & VENDOR STRATEGY

Law-enforcement interoperability.

Enabled investigative information sharing with the provincial police and national police systems within the cooperative's framework.

OFFERED TODAY AS: PUBLIC-SAFETY DELIVERY

Workforce onboarding to a secure system.

Brought the unit's registrar authorities, trainers, and 60+ constables and staff onto the system through a trainer-led program.

OFFERED TODAY AS: CHANGE & TRAINING

SOURCE ARTIFACTS AND DISCLOSURE

Generalized for the law-enforcement and confidential nature of the engagement: security-architecture specifics, vendor names, individuals, and commercial figures are withheld. Drawn from source artifacts held by the practice — the business case, the system summary, and requirements and training records.

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 · **+1 613-600-2803** (Mon–Fri, 9–5 ET) · **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.