OVERCOMING BARRIERS TO INTEROPERABILITY

Derived from a presentation made by Chief Vince Bevan at the Public Safety Transformations: Technology and Counter Terrorism Conference, April 2004

If you have not yet heard the term interoperability in your workplace discussions about technology, you may be missing a key opportunity to improve your agency’s access to vital operational information. Interoperability is now the way of doing business in many sectors beyond law enforcement such as government, banks and businesses. Interoperability refers to systems that provide trusted, timely and accurate information over a secure network.

Information sharing is just one aspect of interoperability. Within law enforcement, the key is also to build a foundation that provides a climate and infrastructure that fosters cooperation, coordination and communication.

While the public may think that policing services already share information at this level, our experience and results prove differently. Until interoperability is achieved, law enforcement will continue to fight an uphill battle, with organized crime pitted against disorganized policing.

Since 1999, Canada has established the Integrated Justice Information (IJI) Secretariat and Steering Committee, the Data Standards Secretariat (DSS) and, more recently, the National Criminal Justice Index Committee. The collective objective of these bodies is to improve public safety and increase confidence in the criminal justice system.

The DSS published a beta version of the CPSIN Data Dictionary in April 2002, which is the foundation for a powerful, integrated national network linking various sources of information.

At the CACP 2002 Annual General Meeting, members adopted two important resolutions that steer our police services toward achieving interoperability. The first resolution recognized CPSIN as the national standard, and advocated the implementation of CPSIN data standards in the information systems of all partner law enforcement and criminal justice agencies. The second resolution called upon members to pursue interagency agreements for the sharing of operational information.

Common data standards form a basis to achieve information sharing. Standards can relate to data, connectivity, control, security, user interfaces, hardware/software architecture and data communication. Adherence to technology standards minimizes the need to replace existing technology in order to join interoperability partnerships. (Any organization that is in the market for a new system should insist that the vendor provides a product that is compliant). Although technology
standards lower the cost and difficulty of implementing technology-based aspects of interoperability (e.g. wireless communications; information sharing), implementing information sharing may still be costly. But doing nothing can prove to be even costlier. And how do we achieve this goal? A number of steps are involved. Police agencies must be prepared to:

• Define the meaning and goals of interoperability;
• Review relevant legislation and identify perceived barriers to interoperability (e.g. access and privacy laws);
• Develop a governance structure and policy framework;
• Identify business processes that can benefit from interoperability;
• Enhance business protocols to promote a collaborative culture;
• Develop technology standards;
• Establish funding.

Implementing interoperability requires commitment and cooperation among all partners, along with significant resources and significant cultural change.

**Benefits**

The primary benefit is increased operational effectiveness, particularly from an investigative point of view, in that data is now available at an officer’s fingertips. In most cases agencies can participate by leveraging the technology currently in place. These information-sharing partnerships generally do not require an upgrade of the existing record management systems in order to connect.

**Success stories**

In 2001, in an effort to make information sharing a reality, the London Police Service spearheaded implementation of the Law Enforcement Information Portal (LEIP). It was initially aimed at sharing records among three Ontario police services (London, Ottawa and Windsor) that use Versaterm’s Versadex system. A Memorandum of Understanding between the partners governs sharing of information captured in general occurrence reports, as well as data regarding persons, tickets and street checks. The Toronto Police Service has since joined LEIP and other agencies including the Ontario OPTIC consortium and the RCMP are looking to interface their systems. Information-sharing has begun to flourish and soon the Ontario LEIP system will be interfaced with a similar partnership in the Lower Mainland of B.C.

Another success story is the partnership between the Ottawa and Gatineau Police Services, which allows mutual access to RMS. In many cases, suspects live and operate across the Ottawa River and have been able to exploit jurisdictional weaknesses resulting from inter-provincial boundaries. Today, information is readily available between the two agencies regarding suspect location, vehicles and associates. This has proven very useful in our fight against gangs and organized crime; all at the low cost of about $1,500 a year.

Changes in the world over the past decade have transformed the way in which we deliver policing services. In order to better understand our work and the challenges we face, it is vital to access a wide range of information. One of the most important issues facing police services today is the need to share information. We need to put all available information in the hands of first responders as they respond to incidents so they can make informed decisions. The time for discussion and study
has passed. Let's get it done.