Information & Communications Technology (ICT) Committee
Briefing Note - *Shared Services – What Chiefs of Police Need to Know*

Frequently Asked Questions (FAQs) in Regard to Shared Services

The Shared Services concept has become a major thrust of both the federal government and Provincial / Municipal governments. Police Executives understand both the need for long term efficiencies and the difficulties faced by governments in the current economic climate. Therefore they fully support initiatives that make more efficient use of public funds. However, due to the nature of the information that is retained by Police Services, security is a factor that must be carefully researched. The following frequently asked questions (FAQs) will provide Chiefs with important information about Shared Services and assist Police Chiefs in having a discussion with the Shared Services representative with regard to the environment they are configuring.

What is a Shared Service Arrangement?

Shared Services is an arrangement where services that formerly existed in more than one organization are centralized so that one group supplies the service for a number of organizations. For example, Information Technology (IT) services that used to exist in a City, the city Police and in other city Boards and Commissions could be centralized to one IT service in the City. Thus it is called a Shared Service. Although many services could be shared, we will use the example of IT sharing in this FAQ document.

From where do Shared Service Arrangements originate?

The federal government, the government of a province, or a city government usually initiates the move to Shared Services. Governments are under severe pressure to hold the line on tax increases without reducing services. Shared Services is one way that a government may attempt to reduce costs.

Is a Shared Service Arrangement likely to happen in my city?

The idea of centralizing a service holds the possibility of saving money so it is being considered in many cities and provinces and is well underway in the federal government. At some point it is very likely to be discussed by the government that has jurisdiction over your police service.

What will be the intent of the Government when they implement Shared Services?

The intent will be to look at the different services being staffed by your police service and pull appropriate services back to one group within the government (municipal, provincial or federal). Often these discussions involve IT services, however other services can also be considered, such as a centralized call taking and dispatch center that manages police, fire and ambulance calls for service.

How have other chiefs responded to the request?

To simply say that police are “different” and should therefore be excluded from the discussions is unlikely to be accepted. The purpose is to save dollars; dollars which could continue to put officers on the street. So it is important to participate, but there are a number of questions that should be asked before moving your IT (or other) services to a centralized group.

What kind of questions should I ask?

There are many questions that relate to security and operational continuity, so a police service must receive detailed and satisfactory answers to such questions, as well as a well-documented Service Level Agreement (SLA). Some of these questions follow:

Employee Background Checks

How will employees of the Shared Services Provider (SSP), both existing and new, have background checks done, and to what level will the checks be done (many unions refuse to have existing employees submit to a background check)?
How often will background checks be re-done (annual or every two years)?

Security Standards

How will the SSP meet the National Security Standards as Defined in the "*National Police Services Secured Communications Policy 1.1*"?
How will the SSP handle the security that surrounds even email, which is often operational in nature, as opposed to just administrative?
How will the SSP be accredited to allow sharing?
How will compliance with various document security classifications be managed the SSP (The federal Protected A, B, C standard or local equivalent standard)?

Security Breaches

What process will the SSP follow if a security breach occurs?
Will the SSP notify the Chief of Police of the breach and how will this notification occur?
What are the consequences should an employee of the SSP breach security?
Can an SSP employee who has breached security be terminated?

System Availability and Maintenance

How will the SSP provide the availability of systems necessary to ensure officer and public safety?
Since our systems are operational in nature, how will 24-7 up time be guaranteed by the SSP?
How will the SSP handle necessary human intervention on a statutory holiday or granted day off?
How will the SSP governance model allow for the special needs of public safety systems (ex. Friday and Saturday night are common computer maintenance times, however, that is prime time for Public Safety systems)?
What is the SSP governance model to allow for system operation and all functionality during a labour dispute such as a strike?
What number can be called 24/7/365 to report outages and receive assistance?

Application Issues

How will the SSP manage the systems to ensure the chain of evidence and continuity (in many police services continuity is now tracked electronically, and therefore the care and control of such records is a question in the courts)?

Server, Network and Wireless Issues

What will be the role of the SSP in acquiring Servers, desktops, laptops, and other mobile equipment?
What will be the role of the SSP in the in the ever-greening of all computer equipment?
Will the new arrangement be different from what is in place now?
What will be the role of the SSP in providing network services?
Will maintenance of the Voice-Over-IP (VOIP) system be handled by the SSP and how can security of phone calls on a VOIP network be guaranteed?

Service Level Agreements

What list of services is to be provided in the deal?
What sort of Service Level Agreements (SLAs) will be in place to guarantee the provision of services as agreed to by the SSP?
Are penalties built into the SLA if the service level is not met by the SSP?

These are only initial questions to initiate discussion. If a Chief of Police has further questions he should contact the ***CACP Information and Communications Technology (ICT) Committee*** for further information.

Document Updated: January 25, 2012

This document is supplied by:
The Information and Communications Technology (ICT) Committee
Canadian Association of Chiefs of Police