Government of Canada Gouvernement du Canada

700TAG – Technical Advisory Note #3

A survey of US Operational Requirements for a Public Safety Wireless Broadband Network

700 MHz Mobile Broadband for Public Safety - Technology Advisory Group

Public Security Science and Technology

August 30, 2011

Partners: The Technology Advisory Group for 700 MHz Public Safety Spectrum (700TAG) is composed of a collaborative group of technical experts led by Centre for Security Science and includes scientific authorities from the Communications Research Center, and technical experts from Federal/Provincial/Territorial/-Municipal agencies.

Objectives

The objective of this Technical Advisory Note is to inform the Canadian public safety community on the work currently underway in the US to establish Operational Requirements (ORs) for a 700 MHz Public Safety Wireless Broadband Network (PSWBN). The US experience can be leveraged to assist Canada's public safety community to formulate a set of ORs which reflect the Canadian context for governance and operating environments.

US Operational Requirements for the PSWBN

ORs express how a user wants to use the network and how he/she wants to interact with the network. Users in the context of the ORs listed in this TAN are 1st responders and network administrators.

A comprehensive set of ORs for the PSWBN are found in a report published by the National Public Safety Telecommunications Council (NPSTC) in November 2007 in the form of a Statement of Requirements (SOR) [1]. The SOR was developed with a broad spectrum of stakeholders that included first responders, equipment vendors, commercial operators, consultants, and government agencies as part of NPSTC's Broadband Working Group (BBWG).

ORs can also be found in RFIs/RFPs that have been issued by various public safety agencies for 700 MHz broadband wireless networks. RFPs from State of New Jersey [2] and Adams County [3], and an RFI from San Francisco Bay Area [4] were reviewed and the ORs found therein are included in this TAN.

Another body defining ORs in terms of recommendations to the FCC is the Public Safety Advisory Committee (PSAC). PSAC was formed in August 2010 by the FCC with a 2-year charter to advise the Emergency Response Interoperability Center (ERIC) on four aspects of the PSWBN: (i) Interoperability, (ii) Applications and User Requirements, (iii) Security and Authentication, and (iv) Network Evolution. The PSAC is resourced by a cross-section of private industry, F/S/T/L government, academia, commercial operators, and public safety. The PSAC work groups tabled their first reports [5] in May 2011.

The ORs that are outlined in this TAN do not necessarily represent mandatory requirements, although some may be identified as mandatory by various jurisdictions in their RFPs or by the FCC. Since the ORs are drawn from documents that have been written at different times and by different groups, it is possible that the ORs may not be congruent in all aspects. The author has not attempted to rationalize potential disconnects.

The ORs in this TAN are categorized as follows:

1. Interoperability.
2. Coverage, availability, and restoration of broadband services.
3. Network resiliency and reliability.
4. Admission control and security.
5. Priority, QoS, and congestion management.
6. Applications.
7. Network management.
8. Sustainability.

A Partnership Led by Defence R&D Canada – Centre for Security Science

DEFENCE R&D DÉFENSE

Agriculture and Agri-Food Canada • Atomic Energy of Canada Limited • Canada Border Services Agency • Canadian Food Inspection Agency • Canadian Nuclear Safety Commission • Canadian Security Intelligence Service • Communications Security Establishment • Defence Research and Development Canada • Environment Canada • Fisheries and Oceans Canada • Health Canada • Industry Canada • National Research Council • Natural Resources Canada • Privy Council Office • Public Health Agency of Canada • Public Safety Canada • Public Works and Government Services Canada • Royal Canadian Mounted Police • Transport Canada • Treasury Board Secretariat

Canada

1. Interoperability

Interoperability can be defined as the ability for a subscriber to communicate, as authorized, with members of his/her own agency and with members of other agencies, nation-wide and across international borders, while in his/her home network and while visiting other networks. The ORs that impact interoperability are summarized below.

1.1. All PSWBN subscribers shall use a common, open-standards-based technology. That is, Long Term Evolution (LTE), starting with Rel.8 as the first instance.

1.2. While visiting another network, a PSWBN subscriber should be authenticated and have access to his/her home network applications and any application in the visited network as authorized by the visited network's administrator. The subscriber should be made aware of what applications he/she has access to on the visited network.

1.3. While transiting between adjacent networks, the hand-over should be seamless. That is, the session is persistent.

1.4. There should be no cross-charging when PSWBN subscribers roam onto other public safety jurisdictions.

1.5. Roaming of PSWBN subscribers onto commercial networks shall be possible in case of absence of coverage of the PSWBN. Roaming charges may be incurred, subject to agreements between commercial carriers and a national public safety network governing entity [*].

1.6. The PSWBN shall interconnect with legacy networks such as LMR, WiFi, WiMAX, the Public Switched Telephone Network (PSTN), Integrated Services Digital Network – Primary Rate Interface (ISDN-PRI), and cellular voice networks.

1.7. The PSWBN subscriber shall be able to interface with upcoming NG911 systems and to exchange multi-media files with the Public Safety Answer Point (PSAP).

1.8. A PSWBN subscriber shall be made aware of the priority and QoS policy that applies to him/her while in a visited jurisdiction.

1.9. Equipment configurations which are unique to public safety shall be tested and verified by a public safety-oriented testing lab, such as Public Safety Communications Research (PSCR).

1.10. The PSWBN shall provide an interconnection to a satellite gateway.

2. Coverage, availability, and restoration of broadband services.

The ORs in this category deal with the coverage of the radio network, the probability that a PSWBN will have service in the coverage area, and the requirements for restoring service in the eventual case of a catastrophic failure of the network. The likelihood of such a failure is greater in hazardous areas subject to floods, earthquakes, tornadoes, hurricanes, etc. Man-made catastrophes can also occur, which can be willful in nature or due to the deterioration of structures. In all cases the ability to restore broadband services to 1st responders is paramount.

2.1 Coverage and signal availability should be defined at the local jurisdictional level, including in-building coverage. Coverage maps shall be accessible by all PSWBN subscribers. The coverage maps shall be kept up-to-date.

2.2 Availability of mission-critical applications and services should be greater than 99.999% (five nines).

2.3 There shall be pre-positioned caches for restoring communications after a disaster; Cell-On-Wheels (COW), Cell-On-Light-Truck (COLT). Each COW or COLT shall carry an

[*] See §8 for Governance Assumptions

eNodeB, a microwave radio for backhaul, a pneumatically operated tower unit, and power generation equipment.

2.4 Deployable systems shall have satellite reach-back for remote locations.

2.5 95% area coverage probability at cell edge with 768Kbps downlink and 256Kbps uplink, and with 70% cell loading.

3. Network resiliency and reliability

These ORs relate to the ability of the network to continue to operate during failures of equipment and facilities. An important aspect of resiliency is the ability to automatically detect the failures, interpret the condition, select the best mitigating action from among several options, and to execute the action in a timely manner.

3.1 Redundant backhaul links. Each link shall be designed to exceed 99.9999% (six nines) availability.

3.2 Redundant Network Operations Centre (NOC), geographically separated, redundant network connectivity.

3.3 Fail-over shall be to network elements of assured operational readiness. This means that stand-by equipment shall also be monitored.

3.4 Back-up power and generators for levels of autonomy ranging from 8 hours for low value sites to 7 days for high value sites. The classification of the value of sites is the purview of local jurisdictions.

3.5 Adequate supply of spares and easy access to spares. Spares shall be located in non-hazardous zones, ie not subject to earthquakes, tornadoes, fires, hurricanes, etc.

3.6 Ability for regional jurisdictions to operate autonomously in case of failure of the national core network.

3.7 Redundant RF coverage from overlapping cell sites.

4. Admission control and security

Security is one of the most important requirements for the PSWBN, as witnessed by the large number of ORs in this section. Security encompasses several dimensions – only one of which is cyber-security. Physical security and information privacy also require particular attention. Access control and the ability to authenticate a user are other important considerations for securing the PSWBN.

4.1 Only authorized users may physically access the sites.

4.2 Authorized operators shall have access to set users' profiles, priority levels, applications, and services.

4.3 Authorized operators shall have access to equipment configuration settings, failure reports, activity reports, and key performance indicators.

4.4 All actions by authorized users shall be logged and time-stamped. The records shall be maintained and auditable.

4.5 Follow a risk-based framework for assessing risk and vulnerabilities and for developing an end-to-end approach to securing next-gen communication systems, according to International Telecommunications Union (ITU) recommendations X.805.

4.6 Ensure that network services are not disrupted by malicious attacks.

4.7 Ensure the protection and integrity of sensitive data and identities.

4.8 Ensure that security mechanisms do not inhibit interoperability.

4.9 Ensure that security-enabled devices and services are easy to use.

4.10 Ensure that security mechanisms are not detrimental to achieving QoS required for mission critical applications.

4.11 Ensure that security can be tailored to support role-based security and allow local control and management of security, consistent with the overarching security policy.

4.12 When roaming onto commercial networks security shall be enabled by VPN and the session shall be persistent when transiting between the PSWBN and the commercial network.

4.13 PSWBN subscribers shall *not* be permitted to set security parameters. However, the subscribers shall be able to ascertain the security status of the session.

4.14 Encryption shall conform to Federal Information Processing Standards (FIPS) 140-2 AES128, 192, or 256.

4.15 Two-factor authentication shall be required for access to the PSWBN, except for sensors and machine-to-machine communications.

4.16 Access to the Internet shall employ firewalls, virus and intrusion detection, spam filtering, and Denial of Service monitoring tools.

4.17 Mission-critical traffic shall *not* be routed through the Internet.

4.18 Terminals shall allow for complete erasure of all data and crypto keys stored onto the device. The erasure command can be initiated remotely or locally.

4.19 The PSWBN operator shall follow ISO 17799 standard practices for security management.

4.20 It shall be possible for the authorized administrator (ex. Incident Commander) to de-activate a device with immediate effect when necessary.

5. Priority, QoS, and congestion management

The ORs in this section deal with how to manage the condition when the traffic demands exceed the network capacity. With unlimited capacity, there would be no need to consider prioritizing one application or user over another. But, capacity *is* finite and proactive steps must be taken to ensure that during the times when the network is congested, thoughtful and organized measures are in place to deal with the congestion.

5.1 Allocate bandwidth to different applications according to the nature of the event and circumstances. An authorized administrator shall be able to assign priority and bandwidth dynamically for individual applications, individual users, and groups of users.

5.2 Applications shall be aware of available network resources, such as bandwidth, and adapt their functionality according to the availability of such resources.

5.3 PSWBN subscribers in their home jurisdictions shall have higher priority than visiting subscribers.

5.4 Load balancing: it shall be possible to divert bandwidth from sectors with low data traffic to sectors with high data traffic. This shall be accomplished automatically without the intervention of a network administrator.

6. Applications

Only those applications which are tested and approved by a governing entity shall be accessible on the PSWBN. PSAC introduces the concept of “well-behaved” applications – able to adapt their functionality to the network resources which are available.

Some applications are hosted locally and are intended for use within a jurisdiction, while others are hosted nationally for all PSWBN subscribers. For example the National Crime Information Center (NCIC) database is hosted nationally. The following applications shall be supported by the PSWBN:

6.1 Emergency Function. It shall have the highest level of priority when activated.

6.2 Location-based applications such as Automatic Vehicle Locating.

6.3 Commercial Mobile Alert System public warning: federal government broadcasts of imminent threat to life or property.

6.4 Database query, Computer-Aided Dispatch, Records Management Systems, Incident Command Systems, Material Safety Data Sheets, patient information and telemetry

6.5 Welcome “splash” page: Home web portal to local applications and information. There shall also be a web portal for applications and resources that are available in the visited jurisdiction.

6.6 Internet access: local direct access to the internet. Access may be limited in accordance with the policies of local jurisdictions.

6.7 Virtual Private Network (VPN) access to the home servers and high security national databases such as NCIC across untrusted networks.

6.8 Short Message Service (SMS), Multimedia Messaging Service (MMS).

6.9 Video applications: real-time, user selectable multi-rate video.

6.10 File Transfer: mug shots, Graphical Information System (GIS) data, pre-recorded video.

6.11 Biometric, sensor, and telemetry data.

6.12 Voice applications: mission-critical voice as standards are defined and products are developed to support this capability.

6.13 Legacy applications shall be tested and verified prior to being released on the PSWBN.

6.14 One-to-many communications shall be supported, which includes communicating with subscribers within the same jurisdiction and within other jurisdictions.

6.15 User devices shall have the ability to operate as WiFi access points to support connectivity to WiFi-enabled devices.

6.16 User devices shall be capable of hosting VoIP and emulating LMR functions.

7. Network management

The ORs in this section deal with ensuring that the logical and physical facilities are in place to be able to assess the health of the PSWBN. Deep visibility into the network is necessary to understand where improvements can be made. In cases where the infrastructure is shared with a private partner it is especially important to be able to audit the quality of the services that have been contracted from that partner.

7.1 It shall be possible to download software and Operating System (OS) upgrades to user devices over-the-air.

7.2 In case of shared infrastructure with a private partner, it shall be possible for the public safety partner to manage and operate separate logical and/or physical databases on the shared network, such as Home Subscriber Server (HSS), and Mobility Management Entity (MME) servers.

7.3 All service-affecting Operations, Administration, Maintenance, and Provisioning (OAM&P) activities shall require command confirmation to minimize the potential of accidental service disruption.

7.4 The PSWBN operator shall have access to all key performance indicators, usage reports, throughput, IP Detail Records (IPDR), accounting reports, received signal levels for each user device, and failure reports of the network. This shall be for PSWBN subscribers and for commercial subscribers that are authorized to roam onto the PSWBN network.

7.5 All sites shall be remotely monitored: door intrusion, temperature, tower lights, fuel level, battery condition, mains power, smoke, fire, water, humidity, equipment status, etc.

7.6 Network and user information shall be displayed graphically and on topographical and street map layers, showing location of sites with drill-down capability to locate faulty units. Equipment configurations and inventory shall be remotely accessible.

8. Sustainability

The ORs of this category deal with the on-going maintenance of the PSWBN in terms of upgrading the infrastructure and the associated operating procedures.

8.1 The PSWBN must keep pace with the introduction of new commercial technology and, therefore, needs be sufficiently funded on a recurring basis.

8.2 New upgrades shall undergo regression tests to ensure that interoperability and the functionality of applications are not compromised.

8.3 There shall be 24/365 monitoring and availability of call centre and field support staff to maintain the network at the specified level of availability.

8.4 The PSWBN operator shall certify its Quality Management processes to TL-9000.

Governance assumptions

The ORs above are posited within the framework of an assumed governance model. The model has two tiers – (i) a national tier and (ii) regional jurisdictions. This framework provides an operational context for the ORs. A different governance model than the one assumed here would render some of the ORs irrelevant or untenable. The assumptions for the governance model are as follows.

G.1 Interoperability policies and issues are dealt with at the national level. Regional jurisdictions (states, Urban Area Security Initiative regions, counties, etc.) are autonomous and have authority to procure material and services. They would adhere to regulations and guidelines that would be set at the national level.

G.2 The national authority shall be responsible for testing, validating, and approving applications for use on the PSWBN.

G.3 The national authority shall be responsible for negotiating roaming agreements with commercial carriers.

G.4 The national authority shall represent the collective interests of the regional jurisdictions in its interactions with federal agencies such as the FCC.

G.5 The national entity shall define an interconnect strategy and coordinate the RF plans of regional jurisdictions so that networks that grow geographically into each other will not interfere with each other.

G.6 The national entity shall define procedures and policies for Network Domain Security, which is the set of security features that enable nodes to securely exchange signaling and user data.

Outcomes

The US public safety community has invested significant money, time, and effort to define ORs for a PSWBN. Industry experts and experienced practitioners were engaged in inter-disciplinary forums to deliver what can be considered as the summum of their thought leadership in today's ORs. Although the ORs referred to in this TAN are extracted from a sample of the US published work on this subject, they can help springboard the development of a set of baseline ORs for Canada's PSWBN.

References:

[1] NPSTC SOR (Sept.2007)

http://www.npstc.org/statementOfRequirements.jsp

[2] State of New Jersey - RFP (July 2011)

http://www.state.nj.us/treasury/pdf/700MHz_Public_Safety_Network_RFI.pdf

[3] Adams County, Colorado – RFP (Jan.2011)

http://www.adcom911.org/LinkClick.aspx?fileticket=wI-RDwI-zos%3D&tabid=65&mid=396

[4] San Francisco Bay Area Regional 700 MHz Wireless Mobile Broadband Network – RFI (Sept.2009)

http://blog.tcomeng.com/SanJose_BayWEB/UASIdoc/UASI_BayAreaBroadbandRFI.pdf

[5] PSAC Work Group reports (May 24, 2011)

http://www.fcc.gov/encyclopedia/emergency-response-interoperability-center-eric-public-safety-advisory-committee

NOTE: *DRDC Centre for Security Science warrants that this advisory note was prepared in a professional manner conforming to generally accepted practices for scientific research and analysis. This advisory note provides technical advice and therefore is not a statement of endorsement of Defence Research Development Canada, Department of National Defence, or the Government of Canada*

Authors: Claudio Lucente

Scientific Authority:

Approved for Release By:

Dr. Andrew Vallerand, DRDC Centre for Security Science, DSTPS