****

**APT REPORT**

**on**

**TECHNICAL REQUIREMENTS FOR
MISSION CRITICAL BROADBAND PPDR COMMUNICATIONS**

**No. APT/AWG/REP-38**Edition: September 2013

**Adopted by**

**The 15th APT Wireless Group Meeting**

**27 – 30 August 2013
Bangkok, Thailand
*(Source: AWG15/OUT-09)***

**APT REPORT ON**

**TECHNICAL REQUIREMENTS FOR
MISSION CRITICAL BROADBAND PPDR COMMUNICATIONS**

**1. Purpose**

The Purpose of this report is define the technical requirements for mission critical broadband PPDR communications The notion of Public Protection and Disaster Relief (PPDR) is defined in ITU-R Resolution 646 (WRC-03) as a combination of two key areas of emergency response activity:

1. **Public Protection** – dealing with the maintenance of law and order, protection of life and property, and responding to local emergency events – in some countries also referred to as the ‘public safety’ or ‘emergency service’ sector (police, fire, ambulance, etc); and
2. **Disaster Relief** – dealing with a serious disruption of the functioning of society, posing a significant and widespread threat to human life, health, property, or the environment, whether caused by accident, natural phenomena, or human activity, and whether developing suddenly or as a result of complex long-term processes.

Resolution 646 (WRC-03) also outlines the importance of radiocommunications to PPDR agencies, in particular to the text in *considerings c)* and *d)*.

**2. Scope**

The scope of this Report is limited to high-level operational and technical requirements only, by way of guidance to national administrations. It offers only minimal guidance on bandwidth allocations to meet specific national deployment arrangements, reflecting the different local demographics, urban and rural geographies, and consequent structure and size of relevant agencies.

In the context of differing funding and network ownership options, this Report also makes no recommendation in regard to how these operational and technical requirements might be achieved. For example, a mobile wireless broadband PPDR application may be realized either by: a) deployment of a dedicated network; or b) priority access to a public network; or c) a combination of a dedicated network in urban areas and priority access to a public network in all other areas. Further, a dedicated network may be funded and owned by government agencies; or funded and owned by another entity with the network services provided to PPDR agencies under specific contractual arrangements.

The purpose of this Report is to define and recommend a common suite of technical requirements for mobile wireless broadband PPDR communications. It is anticipated that administrations will find this report useful to assist in commencing and guiding their own national discussions and planning activities. The structure of this Report may be useful as a framework for the development of more detailed documents, and to ensure that all relevant issues associated with mobile wireless broadband systems for PPDR applications are subsequently addressed and fully defined.

This Report complements the APT AWG Report 27 on "PPDR Applications Using IMT Based Technologies and Networks"

3**. Background**

Radio communications plays a critical and profound role for information exchange within and between Public Protection & Disaster Relief (PPDR) agencies and interaction with other organizations.

By their nature, PPDR operations gain significant benefit from the ability to access a wide variety of information, including informational databases, access to instant messaging, high-quality images and video, mapping and location services, remote control of robots, and other applications. All of these sources of information can be more efficiently conveyed using wireless IP systems. While it is expected that conventional voice dispatch and co-ordination traffic is also destined to be integrated (via VoIP, or VoLTE) into future broadband PPDR radiocommunications systems, it is noted that there may be a longer-term transition, and that administrations may see a role for mission critical narrowband voice communications for some time yet. In any emergency scenario, the ability of PPDR agencies to react quickly and coordinate appropriate resources will largely determine the final outcome and level of impact on local communities of the emergency.

Moreover, the increasing internationalization of crime, and the wider impact of natural disasters, has also highlighted a greater need of cross-border PPDR coordination and cooperation between countries. So harmonization of technical infrastructure to facilitate greater interoperability between agencies is increasingly seen as a matter of high priority.

The emergence of mobile broadband systems based on standardized IMT technologies (such as LTE) offering high-capacity data, video streaming and multimedia functionality, can significantly benefit PPDR organizations. Such benefits include expanded operational capabilities, greater technical innovation and opportunities for economies of scale, particularly in the area of data and video to augment their communication facilities with broadband capabilities - eventually supplementing current narrowband PPDR voice/data networks.

# 4. System requirements for PPDR multimedia applications

Broadband PPDR applications, such as transmission of high resolution images and video, requires much higher basic bit-rates than current narrowband PPDR technology can deliver.

New demand for several simultaneous multimedia capabilities (several simultaneous applications running in parallel) over a mobile system can only be met by a significant increase in throughput and high speed data capabilities, and simultaneous need for very high peak data rates. Such demand is particularly challenging when deployed in localized areas with intensive scene-of-incident requirements where PPDR responders are often operating under very difficult conditions.

Broadband systems may have inherent noise and interference trade-offs with data rates and associated coverage. Depending on the technology and the deployed configuration, a single broadband network base station may have different coverage areas in the range of a few hundred meters up to tens of kilometers, offering wide variations in scope for spectrum reuse. PPDR agencies of different administrations will have different operational and environmental requirements, which will determine the technologies, topologies, coverage areas, applications or broadband PPDR systems, as well as the business models for their deployment.

Collectively, the high peak data rates, extended coverage and data speeds, plus localized coverage area, open up numerous new possibilities for broadband PPDR applications including tailored area networks as described.

4.1 Support of multiple applications

### Systems serving PPDR should be able to support a broad range of applications.

4.2 Simultaneous use of multiple applications

Systems serving PPDR must be able to support the simultaneous use of several different applications with various bit rate requirements. Some PPDR users may require the integration of multiple applications (e.g. voice and low/medium speed data) over the complete network or on a high speed network to service localized areas with intensive on-scene activity.

4.3 Priority access

As desired by the PPDR organizations, systems serving PPDR users must have the ability to manage high priority traffic and possibly manage low priority traffic load shedding during high traffic situations. PPDR users require either the exclusive use of frequencies or equivalent high priority access to other broadband systems or a combination thereof.

4.4 Grade of service (GoS) requirements

Suitable grades of service should be provided for PPDR applications. PPDR users require rapid response times for accessing the network and sourcing information directly at the scene of incident(s), including fast subscriber/network authentication.

4.5 Coverage and Capacity

The PPDR systems typically aim to provide complete geographic coverage (for “normal” traffic within the relevant jurisdiction and/or area of operation (national, provincial/state or at the local level). Such coverage is required on a continuous basis (24 hrs/day, 365 days/year). Additional resources, enhancing either coverage, system capacity or both may be added during a PP emergency or DR event by techniques such as reconfiguration of networks with intensive use of direct mode of operation (DMO) and vehicular repeaters, which may be required for coverage of localized areas.

Reliable indoor and outdoor coverage, coverage of remote areas, and coverage of underground or inaccessible areas (e.g. tunnels, building basements) are also likely to be an important feature of systems supporting PPDR. Further, appropriate levels of redundancy to ensure minimal loss of operational coverage in the event of equipment/infrastructure failure is also likely to be considered extremely beneficial. In addition, such networks should be designed to maximize spectral efficiency, for example by maximizing frequency reuse.

To date, traditional PPDR systems have not generally been installed inside buildings. Urban PPDR systems are designed for highly reliable coverage of subscribers outdoors, and indoors by direct propagation through the building walls. Sub-systems may be installed in specific buildings or structures, such as tunnels, if penetration through the walls is insufficient. Traditionally and in current practice, narrowband PPDR systems have tended to use larger radius cells. Tradeoffs between coverage, capacity and spectrum reuse against infrastructure cost will likely be a decision for each Administration to consider within their own particular context, noting that some administration may favor a larger cell model for PPDR networks

In modern mobile broadband technologies, such as LTE, the user equipment (UE) are pre-specified to be able to reduce their maximum transmit power and transmission bandwidth configuration in order to meet additional (tighter) unwanted emissions requirements. During emergency situations, ability to access to the full UL transmission bandwidth configuration, all resource blocks at maximum power are required by PPDR user(s) to upload mission critical information to their command and control centers with minimum delay. This function may not be required in all scenarios. This should be achieved without the need to activate the NS\_0X/A-MPR function which will require the UE to reduce its maximum output power

4.6 Reliability of Communication

PPDR applications must be provided on a stable and resilient working platform. Reliability requirements should include a stable and easy to operate management system, offer resilient service delivery and a high level of availability (commonly achieved using redundancy and backup, fall-back and auto-recovery, self-organization). In the event of the network failure or loss of network coverage, Direct Mode Operation between PPDR users is required as an immediate solution for reestablishing communications

4.7 Capabilities

PPDR users require control (full or in part) of their communications, including centralized dispatch (command and control center), and management of access control, dispatch group (talk group) configuration, priority levels, and pre-emption (override other users).

Rapid dynamic reconfiguration of the system serving PPDR is required. This includes robust operation administration and maintenance (OAM) offering status and dynamic reconfiguration. System capability of over-the-air programmability of field units is extremely beneficial.

Robust equipment (e.g. hardware, software, operational and maintenance aspects) are required for systems serving PPDR. Equipment that functions while the user is in motion is also required. Equipment may also require high audio output (to cope with high noise environments), along with special accessories such as special microphones (e.g. lapel, in-ear), operation while wearing gloves, operation in adverse environments (heat, cold, dust, rain, water, shock, vibration, explosive and extreme electromagnetic environments) and long battery life.

PPDR users require the system to have capability for fast call set-up and dialing, including instant push-to-talk operations[[1]](#footnote-1) (internally or to different technologies) or a one-touch broadcasting/group call and Direct mode (also known as talk-around or simplex) operations., PPDR users also require commu­nications with aircraft and marine vessels, control of robotic devices, vehicular coverage extenders (deployable base stations, to extend network coverage to remote locations)

PPDR systems should include a capability for rapid deployment coverage extension, and for a high degree of systems self-management. Further, as the trend continues to move towards IP based solutions, all PPDR systems may be required to be either fully IP compatible or at least able to interface with other IP based systems.

Appropriate levels of interconnection to the public telecommunications network may also be required[[2]](#footnote-2). The decision regarding the level of interconnection (i.e. all mobile terminals vs. a percentage of terminals) may be based on specific local/national PPDR operational requirements. Furthermore, the specific access to the public telecommunications network (i.e., directly from mobile or through the PPDR dispatch) may also be based on the local/national PPDR operational requirements.

4.8 Security requirements

PPDR networks must provide a secure operational environment. Security requirements should include encryption technology, support for domestic encryption algorithms, authentication for users, terminals and networks, user identification and location, air interface encryption, integrity protection against unauthorized intrusion, end-to-end encryption, support for third-party key management center, system authorization management and over-the-air key updating. In addition to these system-level requirements, suitable operational procedures will also need to be developed to accomplish required levels of security for information being passed across the network.

Notwithstanding, there may also be occasions where administrations or organizations, which need special security measures, to interconnect their own equipment to meet their own unique security requirements.

4.9 Cost implications

Cost effective solutions and applications will continue to be extremely important to PPDR agencies, especially if they are responsible for ongoing operational expenses. Therefore, the use of open standards, maintenance of a competitive marketplace, and explicit support for broader economies of scale, will be important issues for consideration by national administrations.

4.10 Performance requirements

PPDR networks must be able to support the following performance requirements: high quality audio (quality and intelligibility), security, images, video, real-time video and ultimately provide the level of availability and data throughput to serve all of the applications enabled by a broadband PPDR capability, to the quality/resolution needed.

This will entail fast dialing and setup of calls, high throughput with adequate guarantees of quality of service, and robustness. These may be accomplished through; reallocation of both uplink and downlink rates (depending on the RAN technology), increasing spectrum efficiency, ergonomic design of terminals, very good signal coverage, high terminal radiofrequency performance, and maximum mobility.

# 4.11 Electromagnetic compatibility (EMC) requirements

Systems supporting PPDR should be compliant with appropriate EMC regulations. Adherence to national EMC regulations may be required across networks, radiocommunications standards and co‑located radio equipment.

# 5 Operational requirements

This section defines the operational and functional requirements for PPDR users.

5.1 Radio operating environments

The overall safety of PPDR personnel can be significantly improved via more functional, more reliable, and more extensive wireless communications systems. Systems supporting PPDR should be able to operate in the various radio operating environments, which are defined as average day-to-day operations, large emergencies or public events, and disasters. These operational distinctions are identified since they have subtly distinct characteristics and may impose different requirements for PPDR communications.

PPDR radiocommunications equipment should be able to support at least one of these operating PPDR environments; however, it is preferable that PPDR radiocommunications equipment support all of these radio operating environments. For any of these environments, information may be required to flow to and from units in the field to the operational control centre and specialist knowledge centers.

Although the type of operator for systems supporting PPDR is usually a regulatory and national matter, systems supporting PPDR may be satisfied by public or private operators, or a combination of the two.

PPDR systems and equipment capable of being deployed and set-up rapidly for large emergencies, public events and disasters (e.g. severe floods, large fires, the Olympics, peacekeeping) are extremely beneficial along with the flexibility to dynamically vary uplink and downlink bandwidth and/or assigned channel capacity.

5.2 Interoperability

Interoperability is an important requirement for PPDR operations. PPDR interoperability is the ability of PPDR personnel from one agency/organization to communicate by radio with personnel from another agency/organization, on demand (planned and unplanned) and in real-time. This includes the interoperability of equipment internationally and nationally for those agencies that require national and international cross-border cooperation with other PPDR agencies and organizations. Various options are available to facilitate communications interoperability between multiple agencies and networks. These include, but are not limited to:

a) adoption of a common technology, such as IMT (e.g. LTE, as in the US);

b) the use of common frequencies and standardised equipment,

c) utilising local, on-scene command vehicles/and equipment/procedures,

d) communicating via dispatch centres and/or system interconnection nodes/devices,

e) utilising technologies such as audio switches or software defined radios. Typically multiple agencies use a combination of options, or

f) interconnection with (via standard interface and open system infrastructure)

* narrowband PPDR systems
* Public communication networks (fixed and mobile)
* Satellite communication network
* Other information systems

However, although the importance of interoperability is recognized, PPDR equipment should be manufactured at a reasonable cost, while incorporating various aspects specific to each country/organization. Administrations should consider the cost implications of interoperable equipment since this requirement should not be so expensive as to preclude implementation within an operational context.

5.3 Compatibility

PPDR networks must provide compatibility with existing network types such as current trunked networks, although the mechanism of achieving this may differ between countries. Compatibility requirements may also include diversity of supply, use of open international standards, backward compatibility, and having a smooth upgrade and evolution path.

5.4 Spectrum usage and management

Depending on national frequency allocations, PPDR users must coexist with other terrestrial mobile users. Detailed spectrum arrangements vary from country to country. Furthermore, there may be several different types of systems supporting PPDR operating in the same geographical area. Therefore, interference to systems supporting PPDR from non-PPDR users should be minimized as much as possible. This is generally achieved through appropriate spectrum planning and frequency coordination at the national level.

# 5.5 Regulatory compliance

Systems supporting PPDR should comply with the relevant national regulations. In border areas (i.e. areas adjacent to other countries), suitable coordination of frequencies should be arranged, as appropriate. PPDR systems supporting that provide extended coverage into neighboring countries should also comply with regulatory agreements between the neighbors.

# 5.6 Planning

Planning and pre-coordination are essential to providing reliable PPDR communications. This includes ensuring that sufficient equipment and backhaul is available (or can be rapidly called upon) to provide communications during unpredictable events and disasters, and ensuring that channels/resources, user groups and encryption keys are pre-allocated for seamless deployment. It would be beneficial to maintain accurate and detailed information so that PPDR users can access this information at the scene.

Administrations have, or may also find it beneficial to have, provisions supporting national, state/provincial and local (e.g. municipal) systems.

**6. Table of Broadband PPDR Requirements**

 Attachment 1 contains an example table of requirements indicating the degree of importance attaching to particular requirements under the three radio operating environments: “Day-to-day operations”, “Large emergency and/or public events”, and “Disasters”. The degree of importance attributed to each requirement may be different between administrations. It is up to the administrations to make a choice regarding the relative importance of these requirements. This table may require future review and updating as mobile broadband technologies evolve.

**7. Examples of PPDR scenarios**

Attachment 2 provides some examples of PPDR scenarios. It is recognised that such scenarios will vary between countries whose requirements may greatly differ. It is intended that more such examples be prepared depicting studies from other countries/members which can then be further appended to the report during its further updating and revision

**8. Summary**

This report provides an outline of the technical requirements of mobile wireless broadband communications systems to meet mission critical broadband PPDR requirements. It presents a high-level framework and broad rationale, along with a fundamental set of recommended operational and functional requirements that might be found useful to regional administrations for a variety of purposes.

A specific objective of this report is to encourage administrations to adopt common technology, technical features and functional capabilities, as well as harmonized spectrum arrangements as far as practicable, to maximize the potential for regional co-operation and cross-border inter-working. Further, pursuit of such harmonization is expected to lead to greater market scale to the benefit of manufacturers/vendors, government agencies, and PPDR management and operational staff.

It is anticipated that this Report will become a starting point for more detailed consideration and planning in each country by relevant administrations aiming to further develop their PPDR agencies according to contemporary operational capability and practices. This Report is not intended to be a specification (minimum or otherwise) for comparative assessment of alternative systems or commercial proposals, or for reference citation in competitive commercial tendering/acquisition documents.

**ATTACHMENT 1**

**Table of technical requirements for mission critical PPDR broadband communications**

|  |  |  |
| --- | --- | --- |
| Technical Requirement | Specifics | Importance[[3]](#footnote-3) |
|  |  | P1 | P2 | P3 |
| Functional | Simultaneous use of multiple applications | H | H | M |
| Integration of multiple applications* Voice, data & video
* Multicast and unicast services
* Real time instant messaging
* Scene video transmission
* Mobile office functions
* VPN services
* Telemetry
* Remote control
* Location of terminals
 | H | H | M |
| Integration of local voice, high speed data and video on high speed networks |
| Priority access | Manage levels of priority in traffic with load shedding during high traffic periods | H | H | H |
| Accommodate increased traffic loading during major operations and emergencies | H | H | H |
| Exclusive use of frequencies or equivalent high priority access to other systems | H | H | H |
| Grade of service | Suitable grades of service to support a prioritized range of services (see Annex 2 below) | H | H | H |
| Guaranteed throughput | H | H | H |
| Rapid response times for accessing network andinformation directly at the incident scene, including fast subscriber/network authentication and session set up | H | H | H |
| Coverage | PPDR system should provide complete coverage within relevant jurisdiction and/or operation | H | H | M |
| Coverage of relevant jurisdiction and/or operation of PPDR organization whether at national, provincial/state or at local level | H | H | M |
| Systems designed for peak loads and widefluctuations in use | H | H | M |
| Enhancing system capacity during PP emergency or DR by techniques such as reconfiguration of networks with intensive use of direct mode operation | H | H | H |
| Vehicular repeaters (NB, WB, BB) for coverage oflocalized areas | H | H | H |
| Very good reliable indoor/outdoor coverage | H | H | H |
| Coverage of remote areas, underground and inaccessible areas | H | H | H |
| Appropriate redundancy to continue operations, when equipment/infrastructure fails | H | H | H |
| RAN shall utilize maximum frequency reuse efficiency.  | H | H | M |
| Capabilities | Rapid dynamic reconfiguration of system | H | H | H |
| Control of communications including centralized dispatch, access control, dispatch group configuration, priority level setting and pre-emption. | H | H | H |
| Network system level management capability | M | H | H |
| Stable & easy to operate management system | H | H | H |
| Robust OAM offering status reporting and dynamic reconfiguration.  | H | H | H |
| Network to perform basic self –recovery, expediting service restoration and a return to redundant operations. | H | H | H |
| Packet data capability  | H | H | H |
| Internet Protocol compatibility (complete system or interface with) | M | M | M |
| Robust equipment (hardware, software, operational and maintenance aspects) | H | H | H |
| Portable equipment (equipment that can transmit while in motion) | H | H | H |
| Equipment requiring special features such as high audio output, unique accessories (e.g. special microphones, operation while wearing gloves, operation in hostile environments and long battery life) | H | H | H |
| Fast session set-up and instant “push-to-talk” operation | H | H | H |
| Communications to aircraft and marine equipment, control of robotic devices | M | H | L |
| One touch broadcasting/group session establishment | H | H | H |
| Terminal-to-terminal communications without infrastructure, (e.g. direct mode operation/talk-around), vehicular repeaters. | H | H | H |
| Rapid deployment capability – infrastructure & terminals | L | H | H |
| The Network shall provide seamless coverage (via handoff/handover mechanisms) and continuous connectivity within the 95th percentile coverage area at stationary and vehicular speeds up to 120 kph.  | H | H | H |
| A single common air interface (CAI) shall be utilized for the mobile broadband network.  | H | H | H |
| Mobile/portable station nominal transmit power shall be 0.25W ERP (24 dBm) and shall not exceed 3 W ERP (34.8 dBm) in rural areas for portable devices.  | L | L | L |
| Support | 24-hour and 7 days-a-week (24/7) support for fixed and user equipment | H | H | H |
| The network operations centre to operate on a 24x7x365 basis | H | H | H |
| 24/7 operations including field based support as necessary to maintain the availability of the network. In all cases, 24/7 access to call centre support for issue resolution and assistance is also required | H | H | H |
| Reliability and adaptability  | Ability to operate in accordance with national EMC regulations | H | H | H |
| Adaptable to extreme natural and electromagnetic environments. No functional network failure during climate events, operational vibration, earthquake, EMI/ESD, and supplied power events. | H | M | L |
| Support operation of PPDR communications in anyenvironment | H | H | H |
| Fixed, mobile & terminal equipment adaptable to a wide range of natural environments, with any physical facilities supporting network equipment meeting contemporary standards for electric surge suppression, grounding and EMP Protection | H | H | H |
| PPDR systems operation in accordance with national EMC regulations | H | H | H |
| Robust network and management system | H | H | H |
| Stable, resilient working platform | H | H | H |
| Self-managed network | H | H | H |
| Coordinated development of business continuity plans. | H | H | H |
| Resilient service delivery | H | H | H |
| High availability design – e.g. Diversity, redundancy, automated failover protection, backup operational processes. | H | H | H |
| Network & operational testing to ensure data/call processing functionality is restored within predetermined and guaranteed time period following an outage | H | H | H |
| The above should result in PPDR broadband networks at least matching the level of robustness displayed by the current public safety land mobile radio (i.e., P-25 or TETRA). | H | H | H |
| Availability | Service availability shall not be calculated to allow a prolonged outage even in one service area. | H | H | H |
| Power backup using battery backup and /or power generation. Redundant backhaul circuits from the RAN to the core and to the base stations. High wind loading for the cell towers (Availability 99.995% at year 10) | H | H | H |
| Highly reliable (99.999%) individual network elements. Ensuring adequate supply and easy access to spares to reduce Mean Time To Repair (MTTR). Operational readiness assured even in a maintenance window. | H | H | H |
| Redundant elements should automatically detect failure and activate to provide service upon failures of primary network components | H | H | H |
| Security  | End to end encryption. The network shall provide cryptographic controls to ensure that transmissions can only be decoded by the intended recipient. This must include data encryption over all wireless links.  | H | H | L |
| Support for domestic encryption arithmetic | H | H | L |
| The encryption should support both point‐to‐point traffic and point‐to‐multipoint traffic.  | H | H | L |
| The network shall support periodic re‐keying of devices such that traffic encryption keys may be changed without re‐authentication of the device and without interruption of service. | H | H | H |
| The network shall provide cryptographic controls to ensure that received transmissions have not been modified in transit.  | H | H | L |
| Access to public safety services and applications shall be provided only to those authenticated users and/or devices as specifically authorized by each PPDR organization. | H | H | M |
| The network shall require each device that attempts to connect to the network to prove its identity prior to granting access to network resources. Each device shall be assigned a unique identifier, and the authentication method must provide strong assurance (e.g. by public key cryptography) of the device's identity in a manner that requires no user interaction.  | H | H | M |
| The device authentication service shall utilize an open standard protocol.  | H | H | H |
| To protect against both malicious devices and malicious network stations, the authentication must be mutual, with the device proving its identity to the network and the network proving its identity to the device.  | H | H | H |
| Each PPDR organization shall be granted the option to require user authentication in addition to device authentication for certain devices assigned to that organization. When user authentication has been selected as a requirement, the network shall require each of the organization's designated devices to prove its user's identity prior to granting access to network resources. | H | H | H |
| For organizations requiring user authentication, the network must facilitate sequential authentication of multiple users from a single device.  | H | H | H |
| System authorization management. Each organization shall be granted control over authorization by means of an administrative interface. | H | H | H |
| For organizations requiring user authentication, the organization shall be granted via administrative interface (e.g. Web based) the ability to add, remove, and manage user accounts that are permitted to access the network. | H | H | H |
| For organizations requiring user authentication, the network must facilitate sequential authentication of multiple users from a single device | H | H | H |
| 3rd party key management system | L | L | L |
| The network shall maintain a record of all device and user access attempts and all authentication and authorization transactions, including changes to authentication and authorization data stores.  | H | H | H |
| Over the air key update | L | L | L |
| The network shall enforce a configurable time‐out, imposing a maximum time that each device may be connected to the network. | H | H | H |
| The network shall enforce an inactivity time‐out, imposing a maximum time that each device may be connected to the network without transmitting data. | H | H | H |
| Each PPDR organization shall be granted control of the network time‐out and inactivity time‐out setting for individual devices assigned to that organization. | H | H | H |
| Each organization shall also be granted via administrative interface the means to manually and forcibly terminate access, including active sessions, to the network for any of its assigned devices individually. | H | H | H |
| The network shall be capable of attack monitoring.  | H | H | H |
| Terminal Requirements for preventing unauthorized use  | Devices shall support the network's device authentication protocol. Each device shall be assigned a unique identifier, and the authentication method must provide strong assurance (e.g. by public key cryptography) of the device's identity in a manner that requires no user interaction.  | H | H | H |
| To protect against both malicious devices and malicious network stations, the authentication must be mutual, with the device proving its identity to the network and the network proving its identity to the device. The device must not permit connectivity to the PPDR network unless the network is authenticated.  | H | H | H |
| Each PPDR organization shall have the option to require user authentication for device access. When user authentication has been selected as a requirement, the device shall require each user to prove his or her identity prior to granting access to applications or network resources.  | H | H | H |
| Devices may support a means of erasing (via best practice multiple pass overwriting of data storage media) all data stored on the device.  | H | H | H |
| Devices may support a means of encrypting data stored on the device such that user authentication is required for decryption.  | H | H | H |
| Cost | Scalable system | L | H | M |
| Open standards | H | H | H |
| Open system architecture | H | H | H |
| Cost effective solution & applications | H | H | H |
| Competitive marketplace for supply of equipment and terminals | H | H | H |
| Reduction in deployment of permanent network infrastructure due to availability and commonality of equipment | H | H | L |
| Implementable by public and/or private operator for PPDR applications | H | H | M |
| Rapid deployment of systems and equipment for large emergencies, public events and disasters (e.g. large fires, Olympics, peacekeeping) | H | H | H |
| Information to flow to/from units in the field to theoperational control centre and specialist knowledge centers | H | LH | LH |
| Operational scenario | Greater safety of personnel through improved communications | H | H | H |
| Intra-system: Facilitate the use of common network channels and/or “talk groups” | H | H | H |
| Inter-system: Promote and facilitate the options common between systems | H | H | H |
| Coordinate tactical communications between on-scene or incident commanders of multiple PPDR agencies | H | H | H |
| Share with other terrestrial mobile users | L | L | M |
| Interoperability | Interoperable/Interconnection with narrowband trunked systems. Interconnection required with:* Inter RF subsystem Interface Voice service and Supplementary services
* Console supplementary Interface Voice service and Supplementary services
 | M | H | H |
| Interoperable/ Interconnection with other broadband systems | H | H | H |
| Interoperable/ Interconnection with satellite systems | H | H | H |
| Interconnection with other information systems | H | H | H |
| Interfaces that interconnect to esoteric systems | H | H | H |
| API compatible with standard interfaces | H | H | H |
| Appropriate levels of interconnection to public telecommunication network(s) – fixed and mobile | M | M | M |
| Spectrum usage & management | Suitable spectrum availability (BB channels) | H | H | H |
| Minimize interference to PPDR systems | H | H | H |
| Increased efficiency in use of spectrum | M | M | M |
| Appropriate channel spacing between mobile and base station frequencies | M | M | M |
| Dynamic spectrum allocation | H | H | H |
| Comply with relevant national regulations | H | H | H |
| Reallocation of upstream and downstream rates | H | H | H |
| Regulatory compliance | Coordination of frequencies in border areas | H | H | M |
| Provide capability of PPDR system to support extended coverage into neighboring countries (subject to agreements) | M | M | M |
| Ensure flexibility to use various types of systems in other Services (e.g. HF, satellites, amateur) at the scene of large emergency | M | H | H |
| Adherence to principles of the Tampere Convention | L | L | H |
| Planning  | Reduce reliance on dependencies (e.g. power supply, batteries, fuel, antennas, etc.) | H | H | H |
| As required, have readily available equipment (inventoried or through facilitation of greater quantities of equipment) | H | H | H |
| Provision to have national, state/provincial and local (e.g. municipal) systems | H | H | M |
| Pre-coordination and pre-planning activities (e.g. specific channels identified for use during disaster relief operation, not on a permanent, exclusive basis, but on a priority basis during periods of need) | H | H | H |
| Maintain accurate and detailed information so that PPDR users can access this information at the scene | M | M | M |

**ATTACHMENT 2**

**EXAMPLES OF BROADBAND PPDR SCENARIOS STUDIED IN SOME APT COUNTRIES**

**Example 1: Scenario of LTE PPDR Broadband contributed by Motorola Solutions India (based on a scenario in USA)**

Given the unique mission critical requirements of public safety, it is essential that first responders have unilateral control over sufficient broadband capacity to serve current and future needs. To this end, Motorola Solutions developed a model to evaluate public safety’s broadband wireless requirements by drawing upon existing policies and recent incident feedback. For purposes of this research, Level 1 through Level 3 Hazardous Materials Incident was considered: Level 1 being a Tanker Spill, Level 2, a Clandestine (Drug) Lab, and Level 3, a Petrochemical Refinery incident. Table 1 below summarizes an example of a public safety equipment and personnel response needed to manage such an incident based on consultation with PPDR agencies in USA.



**Table 1** – Typical Response Scope for Level 1-3 Hazardous Materials Incidents

As is clearly evident in Table 1, even the lowest level incident, Level 1, will elicit considerable response from a variety of public safety agencies that will all arrive on the scene needing broadband services.

The incident scene broadband demands are classified as follows based on usage:

1. **Individual (Person/Vehicle) CAD overhead functions**: The classification includes incident data, GPS information, biosensors and other status, messaging, and queries. Each station individually consumes relatively low down/uplink bandwidth but in aggregate usage can be significant across many users.
2. **Incident Scene database lookups/downloads and information searches**: The classification includes the download of manuals, incident scene images, maps and topography information, building plans, etc. This use case has the unique requirement that, in general, the information is needed quickly as incident commanders initially assess the scene and develop a strategy. The model assumes that all expected initial data is downloaded and available with the first 10 minutes of the incident. The demands are scaled with the incident size and complexity.
3. **Video**: This classification of usage is comprised of personal video cameras for workers operating in the hot-zone, incident scene (car) video positioned around the perimeter, and cameras deployed within the scene. The video is uplinked via the network and a subset of the streams (switchable on command) is down-linked to the on-scene command center. Rates of 400kbps (QVGA 320x240 @ 30fps) and 1.2 Mbps (1280x960 @ 30fps) are used and the number of each type of video stream is scaled with the size and complexity of the incident.

Figure 2 below summarizes the results of the analysis where the bandwidth demands for both uplink and downlink are compared with the expected *average* capacity of a single LTE serving sector (*cell edge* performance, especially on the uplink, would be considerably less and obviously under optimistic conditions peak data rates can be much higher). A “background” load of 20% is added to the total demand assuming this would be a minimum “base load” for other non-incident related, nominal activities across the sector coverage area.



**Figure 2** – Broadband Wireless Capacity Implications

10MHz (5+5) of capacity is insufficient to service the uplink demands for even a Level 1 incident. On the other hand, although 10+10 is still deficient for the ideal Level 3 workload, it services the Level 1 and Level 2 incident demands and comes much closer to providing reasonable capability for the Level 3 case.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Example 2: Scenario of LTE based technology for PPDR broadband provided by China**

This is a study of a typical PPDR incident, a bank robbery, which happened in China. Wireless bandwidth requirements of PPDR agencies in this mission critical scenario are analyzed.

Process to handle the incident:

1. 110 command center receives emergency call and dispatches nearby police officers to the scene.
2. The dispatched police officers contact the command center and ask for the aid of SWAT Police officers in accordance with the situation and set up a command center on the scene.
3. Firefighters and medical team arrive on the scene.
4. Police helicopter arrives on the scene. The helicopter transmits panoramic high definition images to the on-scene command center and the on-scene command center transmits the images through wireless network to remote command center. The remote command center transmits large amount of data concerning the incident and the scene to the on-scene command center, which in turn broadcasts the data to each emergency team.
5. The SWAT Police officers arrive on the scene. They deploy surveillance equipment to conduct covert surveillance and collect information. Critical information is transmitted to the on-scene command center in a manner of high definition images while general information is transmitted through two channels standard definition images. The on-scene command center broadcasts the video images to whichever emergency team that needs the video.
6. The SWAT Police officers deploy remote-controlled reconnaissance robots and transmit indoor video in two manners, high definition and standard definition.
7. Negotiation experts arrive on the scene. To make sure the experts can see and hear every detail of the scene; assistants for the negotiation monitor the negotiation by making full use of videos collected through all equipment.
8. SWAT Police officers make the strategy for strike and ten of them prepare to start the strike. Two head-mounted cameras of standard definition are carried with them.
9. The operation is finished.

Throughout the whole process, the peak spectrum demand happens when the SWAT Police team strike. Only when bandwidth requirement during this period is met, the emergency can be properly handled.

Tests have proved that for video of standard definition, at a distance of about 15 meters, CIF 352×288p, 25fps, only gender, figure, and motions can be identified, whereas D1 704×576p, 25 fps, face, details of figure, and license plate numbers can be identified; for videos of high definition, at a distance of over 30 meters, 720P 1280×720p, only gender, figure, and motions can be identified, whereas 1080P, face, details of figure, and plate numbers can be identified.

Table 1 lists the bandwidth requirements of different personnel and equipment during the strike. Compared to the bandwidth for video transmission, the bandwidth for uploading and downloading voice and data can be ignored. Thus, table 1 only lists the statistics for downlink and uplink bandwidth required by video.

**Table 1 Analysis of Bandwidth Requirements during the Strike**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Emergency Team | Personnel and Equipment | Service(s)  | Source Coding Rate | Uplink Bandwidth | Downlink Bandwidth |
| Command Center | 15 | compressed video broadcast |  |  | 7MHz |
| Ordinary Police Officers | 20 | identity authentication and query |  |  |  |
| Medical Team | 5 | 1 channel D1 video upload and download | 1Mbps | 2MHz | 2MHz |
| Fire Fighters | 5 | 1 channel D1 video upload and download | 1Mbps | 2MHz | 2MHz |
| Negotiation Experts | 3 | high definition video download |  |  | 4MHz |
| Strike Team | 10 | 2 channels CIF video upload and download | 0.5Mbps | 2MHz | 4MHz |
| Police Helicopter | 1 | 1 channel 1080P video upload and download | 3Mbps | 5MHz | 1MHz |
| Reconnaissance Robot | 10 | 1 channel 720P, 1 channel CIF video upload | 3.5Mbps | 6MHz |  |

The above analysis shows that to fulfill the task, uplink needs at least 17 MHz bandwidth and broadcast downlink at least 7MHz (frequency spectrum utilization about 50%). Consider the routine work; extra 10% background spectrum width is needed. The total spectrum width is about 27MHz. It is asserted that the more complex the incident case, the more spectrum is needed.

The bandwidth needed by broadband PPDR would be tremendously different in different scenarios. However, the typical case above shows that allocating about 30 MHz bandwidth for PPDR agencies may fulfill the requirements of PPDR general scenarios, except in disaster relief situations that require more spectrum.

**Example 3: An Example of how PPDR Broadband requirements can be met – provided by Telstra**

With Release 12 due to be published in early 2014, the 3GPP specifications are already well-advanced toward ensuring IMT (LTE) meets the functional requirements of broadband PPDR systems, in accordance with ITU-R report 2033. But to optimize the operational effectiveness of IMT networks for supporting PPDR, deployment and configuration aspects also need to be carefully considered. This Annex outlines an economically efficient means of delivering wide-area, fully functional and high-capacity mobile broadband services to meet the highly dynamic needs of PPDR agencies. Moreover, the strategy also offers a better ‘user experience’ by ensuring that PPDR users remain seamlessly connected throughout a broad coverage area.

**PPDR Mobile Broadband Deployment Options**

To exploit the capabilities of IMT mobile broadband technology, and the utility of assigned radio spectrum resources, PPDR agencies have three options in regard to their network infrastructure:

* Secure an exclusive PPDR spectrum allocation, and build/maintain a dedicated private PPDR mobile broadband network;
* Secure an exclusive PPDR spectrum allocation, and establish a commercial build-own-operate arrangement with another entity to deliver a dedicated PPDR mobile broadband network; or
* Integrate an exclusive PPDR spectrum resource within a broader IMT network, built and maintained by an established operator, to provide an integrated and seamless PPDR user experience. The radio, transmission and core network elements are shared, with options for dedicated authentication and user-management/access functionality under special MVNO[[4]](#footnote-4) arrangements.

These options have already been explored in some depth in some countries, and a summary of the outcomes of one such detailed analysis is summarized in the following sections.

1. **Exclusive PPDR spectrum resources for a dedicated PPDR network**

Given sufficient government financing, this option could be deployed with enough potential capacity and resiliency to accommodate day-to-day operations and most emergency response needs. PPDR agencies would not only have exclusive use of the spectrum and retain direct ownership and control of the network, but could directly manage service levels and determine user authentication and access rights. But a major disaster or terrorist event may still over-burden or extend beyond the reach of such a dedicated network, unless additional capacity or coverage relief measures were made available.

However, analysis indicates that a major disadvantage of this dedicated network option for administrations is the very high cost – including initial and periodic capital outlays, and ongoing regular lifecycle management, operations and maintenance costs. The inherent trade-offs between network scale (coverage), effective capacity and user functionality in a *cost-constrained* environment that has no counter-balancing revenue support, may mean that a smaller network is deployed than might otherwise have been intended.

Moreover, in economic terms, if the network scale is constrained by financing, then the real utility and economic value of the assigned spectrum will also be under-utilized – and the duplication of network investment by government/PPDR agencies and public network operators in major populated areas is economically inefficient, especially if there are alternative approaches available.

The analysis therefore clearly suggested that deploying a dedicated network is likely to be under-funded, fall short of coverage/capacity expectations, and economically wasteful.

PPDR spectrum occupancy

*Unused spectrum*

*capacity*

*Figure 1: Dedicated network using exclusive spectrum*

2. **Exclusive PPDR spectrum resources with a commercial build-own-operate network arrangement**

Similar to Option 1, under this option PPDR agencies retain exclusive use of the spectrum resources, but would no longer build, manage and maintain their own network. Instead, a commercial arrangement with another entity responsible for network build and operation/maintenance, including ownership of the network, would be established. While such a dedicated network would still need to be fully funded, the payments can be more conveniently spread out over time. PPDR agencies can also manage service level agreements and directly influence network scale and ongoing development (subject to available annual finance), and handle user authentication and access rights. Further, by avoiding the large up-front capital outlay, PPDR agencies may be able to financially support a somewhat larger coverage network, possibly with greater capacity, in comparison to Option 1.

The advantages of this approach are: i) potential for improved user experience by leveraging *some aspects* of an existing IMT network (e.g. radio sites and back-haul); and ii) the deferral of the up-front capital costs associated with initial network build – and subsequent network expansions or upgrades – and spreading costs over some longer time period. In addition, ongoing network lifecycle, management and maintenance costs may be lower than Option 1 if PPDR agencies can leverage the network operator’s existing economies-of-scale (for example, leveraging via an existing public network operator). Administration of such a network is also simplified, since the only support staff needed by PPDR agencies are those involved with managing the relationship with the network operator.

However, while this option may be attractive in the short-term, the actual *long-term* cost of such a dedicated and exclusive network will be significantly higher than Option 1 - because the interest (or ‘holding’) costs, that are associated with spreading the capital cost repayments over a longer time period, must inevitably be recovered. Such a cost premium might be considered the ‘cost of exclusiveness’ of the network.

3. **Integrate PPDR spectrum resources within a broader IMT network**

An alternative option, possibly more attractive to many administrations, relies on the ability of IMT networks to ‘partition’ designated spectrum blocks for exclusive use by certain user-groups, such as PPDR agencies – while also sharing the remainder the network coverage, capacity, switching/routing core, backhaul, and radio base-station infrastructure. Moreover, using priority settings available within the IMT technology, and in IP transport layers, a more affordable and effective strategy is available for delivering seamless emergency-grade mobile broadband services over a larger area. The key considerations of the strategy outlined in this Annex include:

* PPDR coverage must be broad – PPDR operational coverage must generally be nationwide (or at least state-wide) for operational effectiveness. While terrorist events or major crime scenes are mostly focused in populated (urban/suburban) areas, natural disasters such as cyclones/tornadoes, tsunamis/floods, volcanic eruptions, and forest fires can strike anywhere – often in regional/rural zones. Public networks may already provide national coverage – but, in any case, extending and ‘hardening’ an existing public network is inevitably easier/cheaper than building an entirely new network of similar scale.
* PPDR functionality must be transparently delivered everywhere – irrespective of geographic location, the full PPDR functionality should be readily/seamlessly available to authorised users. Reflecting the inherent urgency of emergency events and disasters, minimal access delays and latency is critical for ensuring effective response by PPDR agencies. This suggests need for an *integrated* network approach - a simple *roaming* ‘overflow’ scenario is unlikely to meet PPDR user needs for a fast and seamless experience.
* Mobile broadband networks are expensive to build and operate – the cost of building near-nationwide IMT networks ‘from scratch’ with high availability and capacity can be prohibitive – and the ongoing operations and maintenance costs (along with periodic technology upgrades) are a further significant cost burden. Examples of the cost of IMT network build and operation are widely available in the public domain: for example, Telstra’s nationwide 3G HSPA network in Australia, covering 99% of the population and about 27% of the continental landmass of Australia involved an investment of three-and-half-billion dollars (AUD)[[5]](#footnote-5), with an ongoing annual capital investment of hundreds-of-millions of dollars – and a similar level of costs for annual operations and maintenance.
* Sharing public network infrastructure will result in major cost-efficiencies – by avoiding the direct costs of core network, backhaul systems, site access/infrastructure, and Operational Support Systems (OSS), as well as leveraging the public network operator’s procurement scale. There are significant savings and a better user experience through more seamless functionality extending over a larger coverage footprint, for PPDR agencies under an integrated network scenario. While PPDR agencies may require dedicated (MVNO) servers to directly handle user authentication and access rights management, the overall cost of integrating with a public network will be considerably lower than deployment of a dedicated network.
* Enhancing public network resiliency (hardening) is cheaper than building an equivalent new network – while some aspects of a public network may need to be further ‘hardened’, the costs associated with upgrading will always be lower in comparison to deployment of a new dedicated network. This includes items such as: enhanced site back-up power, backhaul link and node redundancy, additional physical and electronic intrusion protection, and other measures. In contrast, however, it is highlighted that some aspects of public network planning offer greater resiliency than traditional PPDR networks: for example, typical public network deployment planning includes overlapping sector-coverage arrangements (coverage ‘depth’) to minimise outages due to loss of a sector – in contrast to the single-layer coverage typically associated with traditional PPDR network planning.
* Leveraging public network infrastructure means faster PPDR deployment – since the majority of network infrastructure is already in place, PPDR services can be put into active service (over a relatively large coverage area) much more quickly – even if further network ‘hardening’ work is still proceeding. This delivers the benefits of mobile broadband to PPDR agencies much sooner than is the case for a dedicated network build.

There are also other important issues that will attract national administrations to Option 3 outlined above, including: i) planning, building and operating an IMT broadband wireless network is not a core skill of PPDR agencies – but public network operators are already fully experienced; ii) the risk of technology obsolescence and future upgrades to keep the network fit-for-purpose is borne by the public network operator; and iii) retention and training of specialist technical staff, vehicles and equipment is no longer required of PPDR agencies, thus reducing agency operating costs.

PPDR spectrum resources

Public network spectrum resources

*PPDR command centre(s)*

*Public network operations centre(s)*

*AAA & other network servers*

*Figure 2: Integrated IMT PPDR/public network sharing RAN, duplicated core, distributed OSS, and configured for partitioned PPDR spectrum and dual HSS/AAA*

**Delivering OPTION 3 – the ‘Lanes’ model**

To deliver emergency-grade mobile broadband services using dedicated PPDR spectrum resources and seamless integration with a public IMT network, a three-stage deployment plan – called the ***L****TE for* ***A****dvanced integrated* ***N****etwork for* ***E****mergency* ***S****ervices* (LANES) model – has been determined as the most appropriate approach:

* Stage 1 – deploy the PPDR spectrum as a ‘partitioned’ (dedicated) resource on existing public network base-station sites, with usage restricted to authorised PPDR users only. The concept is similar to reserving one or more dedicated ‘lanes’ on a public freeway, for exclusive use of emergency services vehicles (*as opposed to building a separate road system exclusively for emergency services*).
* Stage 2 – introduce ‘priority access’ and preferential service levels for authorised PPDR users, to facilitate priority access (‘overflow’) to the public network capacity in times of need (e.g. major event or disaster). This is akin to a mandate that public vehicles must yield to emergency vehicles on the freeway.
* Stage 3 – alongside Stages 1 and 2, progressively enhance the resiliency of the public IMT network in accordance with PPDR agency priorities, to ensure more robust mobile broadband services for users in the event of emergency events and disasters. This is similar to improving freeway lane structure for greater vehicle safety at higher speeds, accommodating specialised emergency vehicles, installing additional entries/exits, way-sides and removable centre barriers, and so forth.

**Emergency Vehicles Only**

**Emergency Vehicles Only**

*Figure 2: The ‘LANES’ Concept for future integrated PPDR Mobile Broadband systems*

Moreover, the concept of ‘partitioned’ spectrum is potentially achievable by two methods: distinct spectrum bands or distinct sub-bands – as illustrated below:

*3GPP Band 28*

*3GPP Band 27*

*3GPP Band 1*

807 MHz

824 MHz

PPDR

852 MHz

869 MHz

PPDR

703 MHz

748 MHz

758 MHz

803 MHz

Public LTE

Public LTE

1805 MHz

1880 MHz

Public LTE network

1710 MHz

1785 MHz

Public LTE network

*Figure 3.1: Example cross-band partitioning*

807 MHz

824 MHz

852 MHz

869 MHz

*3GPP Band 27*

PPDR

Public LTE network

PPDR

Public LTE network

*Figure 3.2: Example sub-band partitioning*

Such spectrum partitioning is intended to provide PPDR agencies with sufficient certainty in regard to network coverage and capacity, to support all day-to-day operational requirements and most emergency events and local disasters.

In the case of an integrated host network employing either cross-band or sub-band partitioning, the introduction of PPDR ‘priority access’ to the public IMT network spectrum enables additional resources to be seamlessly and immediately made available should PPDR traffic levels rise beyond the dedicated spectrum block threshold capacity. In the event of a major disaster, this effectively provides PPDR agencies with immediate and transparent access to considerably greater network capacity than would otherwise be available – while ensuring such economically valuable capacity is not lying idle and under-utilized at other times, as is the case for a dedicated PPDR network.

**Network Capability and Resilience**

To be fully effective, a host IMT network must provide PPDR users with the coverage reach, availability, and overall resilience commensurate with safety-of-life-and-property emergency operations. These three key attributes are inextricably associated with the architecture and configuration of the deployed network, and will involve:

* Sufficient radio base station sites deployed to not only meet coverage objectives, but also to ensure suitable ‘depth’ of coverage in all priority regions;
* Sufficient base-station site physical security and back-up power to maintain operations despite adverse natural events and human attack;
* Backhaul and core network systems configured for redundancy to mitigate any conceivable single-point-of-failure;
* Sufficient security measures and encryption to block unauthorised access or tampering with relevant network servers and routers; and
* 24/7 network status/health monitoring and proactive capacity management to ensure that network issues are immediately addressed before they impact performance or user experience.

The key feature of such measures is that *all of them* can be equally and readily implemented in any network as and where required – irrespective of the platform being a dedicated or shared IMT network. It is noted, however, that a shared public IMT network platform will likely offer possible cost advantages due to the inherently larger procurement scale.

**Device and Terminal Considerations**

A rich eco-system of access devices and user terminals for public/commercial IMT (LTE) systems is already generally available and further developing, in the global market. This eco-system includes a wide range of hand-portable, vehicle-mounted, and OEM device modules.

The PPDR sector has traditionally relied on ruggedized versions of user terminals, along with some special application versions (for example, for helicopter/aircraft, motorcycle, and covert use). Such requirements will no doubt continue to be needed – although possibly not exclusively – so traditional PPDR device/terminal manufacturers will continue to play a central role in this specialized market segment. However, due to unique design requirements, and relatively small market size, special PPDR user terminals may involve somewhat higher development costs, and consequently a higher sales price. Thus, wider harmonization of PPDR spectrum arrangements on a regional (or semi-global) basis will no doubt help to alleviate device/terminal costs – and harmonization is noted as one of the key objectives of the existing ITU-R Resolution 646.

In addition, with the more widespread use of mobile broadband, ‘smart’ phones/devices and tablets will start to play a greater role in day-to-day PPDR operations – encouraging new functions, applications, and methods of working – enabling PPDR agencies to soon realize the benefits offered by economies of scale.

**Conclusions**

The analysis underlying this outline report shows that an integrated approach across spectrum and network infrastructure involving complimentary use of public IMT (LTE) network resources and systems – even with dedicated PPDR spectrum – offers the most cost-effective and economically efficient method of delivering future mobile broadband services for PPDR agencies. It directly delivers the significant benefits of:

* earlier PPDR service availability/delivery;
* wide-area prioritised PPDR network access;
* larger seamless geographic coverage;
* dynamic additional capacity allocation for major events/disasters;
* seamless PPDR user experience across the entire coverage area;
* equivalent levels of resiliency;
* lower costs; and
* greater economies of scale.

In particular, the LANES strategy outlined in this report allows national resources to be efficiently used – and financial investment to instead be directed toward network ‘hardening’, rather than wasteful duplication of existing infrastructure. This strategy also ensures that valuable radio spectrum resources are genuinely and fully exploited to deliver maximum economic and social benefit to the national community. It enables a significantly larger PPDR mobile broadband network to be brought into operation, in a shorter time-frame, and with notably lower project and financial risk to administrations and PPDR agencies.

Leveraging the existing skills and experience of public IMT network operators, further reduces costs, risks and delays associated with bringing advanced LTE mobile broadband technology to assist in maintaining the effectiveness of today’s PPDR agencies.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. APCO Project 16B has defined instant push to talk as <= 500ms for voice call setup [↑](#footnote-ref-1)
2. A description of an international emergency preference scheme (IEPS) is described in ITU T Recommendation E.106. [↑](#footnote-ref-2)
3. The importance of that particular requirement to PPDR is indicated as high (H), medium (M) or low (L). This importance factor is listed for the three radio operating environments:

“Day-to-day operations”, “Large emergency and/or public events”, and “Disasters”, represented by P1, P2 and P3, respectively. The importance levels contained in this column have been based on table included in Report ITU-R M.2033 and have been updated based on input contributions. [↑](#footnote-ref-3)
4. Mobile Virtual Network Operator – equivalent to a private network operating as a closed user group (in this case with exclusive spectrum resource), within a wider commercial network that provides shared core network but with options for separate user authentication and access rights management. [↑](#footnote-ref-4)
5. Moreover, the base station sites, towers, site-shelters, backhaul links and core-network accommodation were already mostly available courtesy of preceding (2G) network investment. [↑](#footnote-ref-5)