December 2015

Considerations for Government Authorities when they are planning to acquire Mission Critical Mobile Broadband Services

Produced by the TETRA and Critical Communications Association
Critical Communications Broadband Group – Strategic Case Group

v 1.01 – Issued 10/12/2015

The Grainger Suite, Dobson House, Regent Centre,
Gosforth, Newcastle NE3 3PF, UK
T +44 (0) 191 231 4328 E admin@tcca.info

Index

Index **2**

Introduction **3**

1. Specification of Services **4**

2. Specification of solution **7**

3. Specification of support organisation **8**

4. Definition of service success criteria and associated penalties **10**

5. Specification of legal conditions, financial strength and ownership **11**

6. Specification of device and application approvals and catalogue **14**

7. Specification of security measures **15**

8. Specification of testing and approval process of the Solution **16**

9. Specification of services at termination **17**

10. Definitions and abbreviations **18**

Introduction

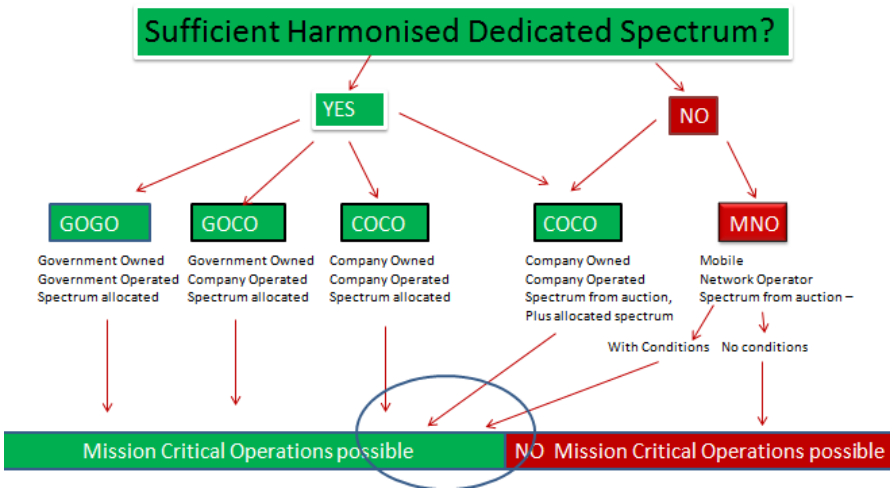
'Mission Critical' in public safety is defined as a function that is extremely important or necessary for a public safety organisation, emergency agency, first responder, etc. to operate successfully and efficiently, and whose failure leads to catastrophic degradation of service that places public order or public safety and security at immediate risk.

Public protection and disaster relief (PPDR) refers to responsible agencies and organisations dealing with maintenance of law and order, protection of life and property and emergency situations.

Some governments in Europe have experience with outsourcing the delivery of Mission Critical communications service and in almost all cases it has been undertaken by specialist service providers who work in partnership with Government organisations to deliver and operate the required services. The concept of a totally owned and dedicated infrastructure for Mission Critical Services is changing with a new approach where sharing with commercial mobile providers is being considered more and more. Whilst anything from a technology perspective is possible the need to ensure the correct guarantees on quality of service, availability and coverage is vitally important.

Mission critical communication is not just the domain of the law enforcement and the emergency services. Those responsible for the Critical European or National Infrastructure such as Gas, Electricity, Water, Transportation, Fuel and Petrochemical also need communications services that can withstand natural and man-made disasters.

There are many different ways of delivering these services and the question of how such essential services can be provided is highly political. A Government may build a dedicated network with the functionalities required by its emergency services, or may outsource to a commercial operator. Combinations of these approaches may include equipment and site sharing, spectrum sharing or simply buying capacity on a network through the MVNO model. But the political questions are more difficult to deal with. Will a government want to have full control over such essential services, or is it satisfied with leaving it to market forces?



This paper focuses on the situations in the circle and aims to highlight some of the considerations both for the users requiring any future mobile broadband service and the actual service providers and mobile operators who will take on the future delivery of these services.

1. Specification of Services

Mission critical communications solutions are used, amongst others, by law enforcement and emergency services in public protection and disaster relief (PPDR) operations, where the reliability, availability, stability, security, capacity and general performance of the solution is of vital importance. Mission critical communication solutions include hardware, software and applications, as well as radio frequency band capacity to transmit and share information between frontline officers and command and control centres.

A specification for services to be purchased should therefore at least include:

a. Coverage

i. The Provider shall meet the following coverage requirements with a statement of availability in % and margins used:
   1. Urban (mobile and portable);
   2. Rural (mobile and portable);
   3. Indoor including indoor penetration loss used;
   4. Air 2 Ground;
   5. Maritime.

b. Capacity demands

i. The Provider shall offer following user capacities at cell edges:
   1. Xx Uplink / yy Downlink
   2. Definition and listing of high-capacity areas;
   3. Definition and listing of lower-capacity areas;
   4. Incident areas.

ii. The Provider shall specify which contention methods will be used
   1. ie. Prioritisation;
   2. ie. Maximum expandable capacity.

iii. Contention Ratio – Minimum throughput per user:
   1. High-capacity areas;
   2. Lower-capacity areas;
   3. Incident areas;
   4. Air to ground;
   5. Maritime.

iv. Control rooms:
   1. Quantity of rooms;
   2. Mobile control rooms;
   3. Seats per room;
   4. IP Connections;
   5. Capacity e.g. steady state and busy hour / major incident user numbers.

c. Stability

i. The Provider shall offer:
   1. Dual coverage from two or more sites to ensure resilience;
   2. No single point of failure in the network;

3. Failure and repair statistics in the form of MTBF – MTTR per infrastructure component.

d. Functional features

i. Data (non-video):
   1. Point-to-point;
   2. Point-to-multipoint;
   3. Intranet and Internet connections;
   4. Internet of Things (IoT) / M2M;
   5. Real time transfer;
   6. Store and forward / push / pull.

ii. Voice:
   1. Group Call (commonly called 'all informed net' and 'talk group call');
   2. Pre-Emptive Priority Call (Emergency Call);
   3. Call Retention;
   4. Priority Call;
   5. One to one (private) call
   6. Ambience Listening;
   7. Call Authorised by Dispatcher;
   8. Area Selection;
   9. Late Entry;
   10. Direct Mode (ProSe), repeater and gateway functionalities as important coverage extension solution using Provider's licensed spectrum and public safety spectrum when not under network coverage.

iii. Video:
   1. Video Point-to-point;
   2. Video group communication (See what I see);
   3. Video feed: uplink video transmission from user to dispatcher;
   4. Video broadcast: broadcast a video file or a video from one user on the field (chosen by dispatcher);
   5. Video consultation,: allow a user to view a video with video recorder functionalities;
   6. Video data notifications;
   7. Remote control of a camera (reuse of already existing standards);
   8. Adaptation to different users/terminals resolution and transmission rates;
   9. Multiple video streams management in one operation.

e. Network management:

i. The Provider shall document his approach to
   1. - Fault Management;
   2. - Configuration Management;
   3. - Account Management;
   4. - Performance Management;
   5. - Security Management.

ii. The provider shall provide the user groups with tactical management.

f. Software:

i. The Provider shall offer to make licenses available of all software needed for the users to utilise the features in the network;

ii. Billing software.
iii. Management software

g. Gateways or other means of 3rd party connections to be based on open standards:

i. Telephony;
ii. IP;
iii. Voice recording;
iv. Data logging;
v. Lawful interception;
vi. Network Monitoring (RAN, BTS, Devices);
vii. Traffic data;
viii. Roaming with / into / from other PPDR organisations / networks.

h. Security

i. Security measures must provide the way to secure authenticity and non-repudiation of transferred information. They shall cover all aspects of hardware, software and staff.
ii. The Provider shall comply with ISO 27001 and provide protection against:
    1. Eavesdropping;
    2. Interception;
    3. Masquerading;
    4. Manipulation;
    5. Replay;
    6. Traffic analysis.
iii. Physical Security:
    1. The Provider shall ensure that all infrastructure assets are physically secured. The level of perimeter security shall reflect the importance of the assets to the service including CCTV, Intruder alarms, Access locks, temperature control, fire and smoke detection.
iv. The Provider shall document the history of access to each site.
v. Jamming and Interference:
    1. The Provider shall ensure that the solution is always available.
vi. The Provider shall isolate the Mission Critical communication information from the overall network so that non-mission critical users and the staff maintaining the general network have no access to the Mission Critical communications.

i. Future upgrades

i. The Provider shall make a test environment available for upgrade procedures, testing and development.
ii. The Provider shall continually upgrade all network elements to the latest versions of standards being used.

j. Standards

i. The Provider shall base his offer on publicly available open standards with licensing under Fair, Reasonable and Non-Discriminatory (FRAND) conditions.

2. Specification of solution

The nature of the service is so essential to the nation, that a detailed description of how a solution is going to be provided is required. As a minimum detail is to be provided on:

a. **Network architecture**
   i. Network components description and interconnections;
   ii. Confirming compliance with applicable European / national standards development organisation(s) standards i.e. ETSI;
   iii. Frequency bands to be utilized for the solution;
   iv. Specification of radio sites;
      1. 8 hours of battery backup;
      2. Protection against vandalism;
      3. Access control;
      4. Backhaul methods and redundancy.
   v. Documentation of end-to-end latency;
   vi. Interference modelling and mitigation.

b. **Coverage**
   i. Prediction methodology;
   ii. Mapping and clutter data;
   iii. Calculation of link budgets;
   iv. Field testing.

c. **Capacity**
   i. Prediction methodology for individuals and groups;
   ii. Traffic handover between frequency bands;
   iii. Field testing.

d. **Redundancy**
   i. No single point of failure documentation;
   ii. Dual backbone;
   iii. Overlapping BTS connections diverse routing.

e. **Resilience**
   i. e.g. Overlapping RAN coverage from different sites;
   ii. e.g. Base station site trunking fallback / eNB IOPS;
   iii. 8 hours of battery backup on RAN sites;
   iv. 98% geographic coverage to mobile units for 7 days in the absence of mains electricity supply.

f. **Interfaces and gateways**
   i. Capacity and limitations;
   ii. Access to interfaces through documented, licensable APIs.

g. **Security**
   i. Inherent encryption;
   ii. Additional over the top encryption;
   iii. Compliance with ISO 27001.

h. **Test methods, conformance tests**
   i. Methods to prove compliance with the specifications.

3. Specification of support organisation

The Provider shall establish a support organisation deemed capable of meeting the authority service requirements. Demands, services and conditions will be the same whether the Provider or one of his sub-contractors are involved in the provision.

The Provider's support organisation shall throughout the whole contract period be able to operate, maintain and meet all requirements in the contract.

The Provider shall establish a specific Network Management Centre staffed for 24/7/365 operation. The task is to ensure continuous supervision of service and provide hotline support service to user organisations.

a. Responsibilities

i. Network management, operation and maintenance;
ii. Network topology planning;
iii. Capacity planning and optimisation;
iv. Life cycle evolution planning;
v. Contract administration;
vi. Administration of security including staff clearance under the rules of the respective National Security Agency/Administration;
vii. Reporting;
viii. Coordination of the operation (predictive maintenance);
ix. Support to end user organisations;
x. Web site;
xi. Connection of users to the service;
xii. Make a test environment available for the duration of the contract;
xiii. Creation of code of connection rules for devices, applications, 3rd part interfaces;
xiv. Administration of a restricted app store with approved app's.

b. Organisation

i. It shall be a well structured organisation following
    1. ITIL methodology and best practice.
    2. ISO:27001 - Information Security Management;
    3. ISO:20000 - IT Service Management;
    4. ISO:9001 - Quality Management.
ii. Information (CV) of the responsible officers. (These cannot be changed without approval by the authority overseeing the Providers contract.)
iii. Details of resource numbers and grade to provide the service.
iv. The organisation shall provide the services 24/7/365.

c. Security

i. The Provider shall ensure that access to the Service is secured and controlled according to Security Operating Procedures;
ii. Security officer details;
iii. Premises access control;
iv. Management of data;
v. Staff clearance and vetting;
vi. The Provider shall establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System (ISMS) derived from the ISO 27001 Standard that is applicable to all the

information, systems and locations and is based on the Plan-Do-Check-Act ("PDCA") methodology;

vii. The Provider shall deploy a protective security monitoring system to capture and securely log all security incidents for audit purposes;

viii. The Provider shall ensure that the operative production network is completely isolated from services produced.

d. Reporting.

i. Real Time access for PPDR staff to network status and traffic behaviour via a secure web service;

ii. Dynamic reporting of specific network behaviour;

iii. Proactive and ad-hoc reporting of network behaviour that might influence PPDR operations;

iv. Historical reporting where the Provider will report on

1. the network behaviour including downtime on each component in the system;
2. all contacts from user organisations;
3. the nature of the contacts and the resulting actions;
4. any change in the infrastructure;
5. SLA's;
6. All security breaches.

v. model/ sample of reporting;

vi. Business Intelligence tools enabling development of needed reporting.

e. **Coordination.** The Provider is responsible for

i. Constant supervision of the network;

ii. Network topology planning;

iii. Capacity planning and optimisation;

iv. Life cycle evolution planning;

v. Maintenance;

vi. Fault correction;

vii. Support to user organisations including immediate activation and de-activation of devices.

f. **Help desk 24/7**. The Provider shall provide

i. Efficient answering and mitigation service;

ii. Specific expertise to manage the service.

g. Web site

i. The Provider shall create, maintain and run a web site with public and secure compartments. The secure compartments shall give access to real-time network statistics;

ii. The Provider shall ensure that the operative production network is completely isolated from services produced;

iii. The web site shall be available 99,99% per year.

h. Application support and certification

i. Authority vetted application providers shall have access to a test environment where applications can be tested and certified.

ii. The Provider shall make relevant staff available on an agreed per hour fee.

4. Definition of service success criteria and associated penalties

This section describes the success criteria that are being contracted and the penalty regime.

a. The list of SLA's for the different kind of services enters into force from acceptance of each geographical area and as users are using it operationally.
b. SLA is measured on a monthly basis.
c. SLA for the overall service is
    i. 99,99 % annually
    ii. 99,9 % monthly
d. SLA in case of reduced service
    iii. Reduced coverage
    iv. Reduced capacity
e. SLA on component level
    I. Essential components shall have 99,999 % uptime
f. SLA on Quality of Service (QoS)
    I. Metrics
    II. Key Performance Indicators (KPI)
    III. Acceptance thresholds
g. SLA on maintenance and repair
h. SLA on Web site accessibility
i. SLA on help desk
j. Penalty is calculated monthly and will be up to xx% of monthly fee.

5. Specification of legal conditions, financial strength and ownership

a. **Legal Conditions:** The purpose of this section is to assist Providers in their understanding of what specific legal frameworks will be used. The term "governmental customer" here means all PPDR organisations or their "mother/daughter/umbrella/joint" organisation responsible for contracting with the Provider.

   i. Parent Company guarantee (PCG)/Performance Bond (PB): (a) PCG – The Provider's parent company agrees to meet the Provider's financial and/or performance obligations should the Provider fail to do so. (b) PB – The Provider provides the government customer with a performance bond usually valued at between five and ten percent of the contract price. The government customer can redeem the bond if the Provider fails to meet its contractual obligations (even if the financial costs of the failure are lower than the value of the bond).

   ii. Intellectual Property: The Authority managing the Provider contract is to have access to relevant IPR under FRAND conditions.

   iii. Liability: Government customer contracts may not include a waiver of consequential and indirect damages. Light breaches will in some countries result in liabilities in the order of 500 M€.

   iv. Open Book Accounting: The government customer has access to the Provider's financial records in order to see any reduction in the Provider's costs in performing the contract. If costs have reduced, the Provider and government customer will split the "profit". Sometimes the split is 50/50 although it is not uncommon for the government customer to receive the majority of any such profit. There is also the possibility to define an upper limit on the profit margin a Provider is allowed to make.

   v. Most Favoured Customer: The government customer must have the best price. The Provider cannot – for a defined period - sell the same (or similar) products and services to another customer at prices lower than those paid by the government customer.

   vi. Step-in: The government customer has the first right to take over the performance of the contract in certain circumstances. For example, where the Provider suffers an insolvency event (e.g. insolvency, arrangement with creditors, etc) or commits a material breach of the contract. The Provider is not paid during step-in, and may also have to meet the government customer's additional costs associated with step-in. The government customer may hand back the services to the Provider, or terminate the contract.

   vii. Termination: The government customer has extensive rights to terminate, often including termination for convenience. Whereas the Provider will only be permitted to terminate in very limited and predefined circumstances (for example, protracted failure to pay undisputed fees).

   viii. Change of Control: A change of control of the Provider will be subject to the government customer's approval, which often may be withheld at

the customer's absolute discretion. In some instances, changes of control are prohibited altogether. A proposed change in shareholder may give the governmental customer the right to step-in (and buy) the questioned amount of shares.

ix. Financial Strength: The Provider is required to show financial strength on a regular, ongoing basis. If the Provider's financial strength diminishes, the government customer may terminate the contract.

x. Control over performance: This is typically very stringent in government contracts – the government customer takes a more involved role than is usual in other contracts, for example in testing and acceptance procedures.

xi. Liquidated Damages/Service Credits: Although they can vary from contract to contract, LD/SC regimes are often more onerous with government contracts as the government cannot allow or afford the project to fail or be delayed, or services to be compromised.

xii. Force Majeure: Force Majeure Events are often defined much more narrowly than in commercial contracts. For example, industrial action is usually excluded from government customer contracts (although sometimes permitted if it is nation- or industry-wide). Force Majeure clauses may also include a proviso that, due to the very sensitive purpose of the contract (i.e. safety of the public), a circumstance will not be considered a Force Majeure event if the party invoking that event reasonably ought to have taken into account when the contract was signed.

xiii. Export Control – A company is responsible for ensuring its products are not exported to prohibited countries. This responsibility extends to onward sale by the company's customers. Government customers will not accept such restrictions imposed on it by another government. Accordingly, standard export control provisions are routinely excluded from government customer contracts.

xiv. Source Code Escrow: The Provider must place the system source code into escrow with a third party, at the Provider's cost. The source code can be released to the government customer in specified events such as insolvency of the Provider, breach of contract by Provider, etc.

xv. Assignment: The Provider is usually not allowed to assign the contract without the government customer's prior consent, which may be withheld at the customer's discretion.

xvi. Security Clearance: The government customer may require certain Provider employees (e.g. those who have access to certain customer sites) to undergo national security clearance.

xvii. Data: Recording and retention obligations for data processed under government customer contracts may be subject to specific data protection legislation.

xviii. Continuous Improvement: The Provider must improve the operation of the system over time at no additional cost to the government customer. New services will be chargeable.

xix. Taxes: Contractual obligation on the Provider to regularly pay its taxes and social security fees/taxes for employees. All laws have to be complied with. Employing illegal workers is a breach of contract. Failure to do so would amount to breach of contract by the Provider.

xx. Confidentiality – Government customers are usually reluctant to agree to standard confidentiality provision, preferring to use their own.

b. **Financial strength of the Provider:** The purpose with this section is to inform the Provider of the requirements the Authority has to his future Provider:
    i. The Provider shall declare his credit rating (AA or better) from a mainstream credit rating bureau.
    ii. The Provider shall maintain the same rating throughout the provision of the services.
    iii. Credit rating evidence needs to be provided twice a year.

c. **Ownership of the Provider:** The purpose with this section is to inform the Provider of the requirements the Authority has to his future Provider:
    i. The Provider cannot change ownership without prior approval.
    ii. The Provider shall deposit the management of the shares with the Authority that manages the Provider contract.

6. Specification of device and application approvals and catalogue

The purpose of this section is to assist Providers in their understanding of how devices should be approved and catalogued.

a. Device Approvals

i. All devices connected to the service provider's network as part of the Mission Critical Service will be pre-approved by the Provider to meet user requirements on interoperability, standards conformance, security, functionality, storage of data, security and size, weight and power.

ii. The Provider shall install and operate a test and certification environment

iii. Device manufacturers pre-approved by the government customer, e.g. resulting from a tender procedure, shall have access to a test environment where devices and accessories can be tested and certified by the Provider, e.g. for interoperability, standards conformance and security.

iv. The government customer shall have similar access, for testing user requirements.

v. The Provider shall make relevant staff available on an agreed per hour fee to be paid by the device manufacturer.

vi. The Provider shall treat all pre-registered device manufacturers equal.

b. Device Catalogue

i. The Provider will maintain an inventory of approved types of devices in the form of a catalogue.

ii. The Provider shall undertake competitive tendering of devices enabling user organisations to procure directly from the Provider.

iii. Alternatively the Provider shall support a National Procurement agency that undertakes competitive tendering of devices enabling user organisations to procure directly from the device vendors.

c. Application approvals

i. All applications used on the Provider's network as part of the Mission Critical Service will be pre-approved by the Provider to meet user requirements.

ii. All applications used on the Provider's network as part of the Mission Critical Service will be pre-approved by the Provider as required for interoperability, standards conformance and security.

iii. Authority vetted and funded application providers shall have access to a test environment installed and operated by the Provider where applications can be tested and certified.

iv. The Provider shall make relevant staff available on an agreed per hour fee to be paid by the app manufacturer.

d. Application "store"

i. The Provider will maintain an inventory of approved applications in the form of a secure web based catalogue or "store" or similar;

ii. The Provider has to take measures that only PPDR users get access to the PPDR "AppStore";

iii. The governmental customer's users should be able to access and download applications from their devices in a controlled manner.

iv. The Provider shall manage the payment of 3rd party applications accessed via the "store".

7. Specification of security measures

The Provider shall establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System (ISMS) derived from the ISO 27001 Standard that is applicable to all the information, systems and locations and is based on the Plan-Do-Check-Act ("PDCA") methodology. As a minimum the following controls should be followed:

a. Provide a security plan structure of procedures and definitions
b. maintain control and inventory of authorized devices;
c. maintain control and inventory of authorized software and applications;
d. develop and roll out secure configurations of hardware and software;
e. continuous vulnerability assessment and mitigation;
f. defend against malware and viruses;
g. monitor application software vulnerabilities;
h. undertake wireless device control;
i. maintain and test a data recovery strategy and solution;
j. provide secure configurations for network devices;
k. limitation and control of network ports and protocols;
l. control of administrative privileges;
m. establish multilayer boundary defences;
n. carry out monitoring and analysis of security logs;
o. implement "need to know" controls;
p. implement user account administrative controls;
q. manage and control data flows;
r. implement and test incident management strategy and solution;
s. carry out security architecture assurance; and
t. carry out periodic penetration testing;
k. premises access control;
l. protection against vandalism;
u. video surveillance of premises;
v. report on all security breaches.

8. Specification of testing and approval process of the Solution

The Provider shall undertake an approval process which will enable the Authority managing the contract to accept the solution and enable the end-user organisation to adopt the service. As a minimum the Provider will:

a. **Undertake a build & approval phase** consisting of:
    i. Test specifications
        1. Coverage
        2. Capacity
        3. Features
    ii. Approval process of tests taking into account
        1. traffic distribution;
        2. load models;
        3. etc.
    iii. Review process of tests
    iv. Review of network architecture
    v. Functional tests
    vi. Basic coverage test.

b. **Complete a Pilot phase** consisting of:
    i. Review of coverage plan
    ii. Design review of network
    iii. Review of support organisation.

c. **Business as usual phase** consisting of:
    i. Test facility for the 3rd party interfaces, device testing and application testing
    ii. Reporting on SLA's
    iii. Calculation of penalties

9. Specification of services at termination

The Service is a vital part of the mission critical users' operations. For that reason it is imperative that the transition to another service provider on termination of the contract will be carried out responsibly, without interruptions and with high requirements for secure and stable operation. As a minimum the Provider will:

a. Produce a full Exit Plan within two months of commencement of the service.
b. Ensure the orderly transition of the Services from the Provider to the Authority and/or any Replacement Provider in the event of termination or expiry of this Contract.
c. Appoint an appropriately skilled, knowledgeable and experienced Exit Manager
d. Provide all reasonable assistance that the Authority may require in connection with any re-tendering process in order to ensure a fair future procurement.

At point of notice of termination and at the start of the procurement the Provider is to supply:

a. Details of the Service(s) including information, manuals, and data in the possession or control of the Provider;
b. the Asset Register;
c. Details of and information relating to the use of the Assets including technical specifications and configuration data;
d. An inventory of Authority Data;
e. Detail on the transition of services to the new Provider including a detailed description of both the transfer and cessation processes.

During the Termination Period the Provider will continue to provide the Services until they are transferred in a satisfactory way to the new provider.

10. Definitions and abbreviations

APP	Application
CCBG	Critical Communications Broadband Group. A working group of the TETRA and Critical Communications Association
CCTV	Closed Circuit Tele Vision
BTS	Base Transceiver Station
DGNA	Dynamic Group Number Assignment
ETSI	European Telecommunications Standards Institute
FRAND	Fair Reasonable and Non Discriminatory
ISMS	Information Security Management System
ISO	International Standard Organisation
ITIL	Information Technology Infrastructure Library
LTE	Long Term Evolution
MCMBB	Mission Critical Mobile Broadband
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MCPTT	Mission Critical Push To Talk
MVNO	Mobile Virtual Network Operator
PCG	Parent Company Guarantee
PDCA	Plan do Check Action
PMR	Private Mobile Radio
PPDR	Public Safety and Disaster Relief
RAN	Radio Access Network
SLA	Service Level Agreement
TCCA	TETRA and Critical Communications Association (see www.tandcca.com)
TETRA	Terrestrial Trunked Radio - a digital trunked mobile radio technology