Nationwide Interoperability Framework

Emergency Response Interoperability Center (ERIC)

Public Safety Homeland Security Bureau

Federal Communications Commission

PSCR, Boulder, CO

Dec 2, 2010

History

- **BBTF Recommendations.** In Sept 2009, NPSTC Broadband Task Force (BBTF) published its recommendation on minimum requirements for roaming and interoperability - the Bureau sought comment on NPSTC BBTF and PSST technical recommendations.
- **ERIC.** On April 23, 2010, the Commission issued an order to establish Emergency Response Interoperability Center (ERIC).
- **Waiver Order.** On May 12, 2010, the Commission granted, with conditions, 21 waiver Petitions.
- **Technical PN.** On May 18, 2010, the Bureau sought comment on technical interoperability.
- **Interoperability Showing.** On May 21, 2010, the Bureau offered further guidance on completing the interoperability showing – later the Bureau tolled the 60-day deadline.
- **Additional Waivers.** On Sept 15, 2010, the Bureau sought comment on additional petitions for waiver.
- **Narrowband Flexibility.** On Sept 28, 2010, the Bureau sought comment on the feasibility of allowing for flexible use of the 700 MHz public safety narrowband spectrum – Comments due Dec 3, 2010.

Broadband Network Strategy

Vision: For significantly less than what has been spent on narrowband interoperability, a new interoperable broadband network will be deployed using commercial technologies, bringing public safety communications into the 21st Century.

National Broadband Plan (NBP) recommends a three-pronged approach to allow the speedy and cost-effective deployment, operation and continued evolution of such a network.

- Creation of an administrative system ensuring that users of the public safety broadband spectrum have the capacity and service they require for their network; they also should be able to leverage commercial technologies to capture economies of scale and scope.
- **Creation of an emergency response interoperability center focused on ensuring that first responders nationwide can communicate with one another via public safety wireless broadband communications.**
- Creation of a grant program to help fund the construction, operation and evolution of the hardened, high-coverage public safety broadband network.

ERIC's Primary Mission

To establish a technical and operational framework that will ensure nationwide operability and interoperability from the outset in deployment and operation of the 700 MHz public safety broadband wireless network.

ERIC's Functions & Committees

- Adopt technical and operational requirements and procedures to ensure a nationwide level of interoperability.
- Coordinate the interoperability framework of regulations, license requirements, grant conditions, and technical standards with other entities.

- **TAC:** On June 20, 2010, the Bureau appointed twenty members to the Technical Advisory Committee (TAC) to advise ERIC on technical matters. Each appointee is either a federal official, an elected officer of a state or local government, or a designated employee authorized to act on behalf of such an officer.
- **PSAC:** On Aug 18, 2010, the Commission released a public Notice seeking nominations for Public Safety Advisory Committee (PSAC) to advise ERIC on various policy and technical matters. Members from state and local public safety agencies, public safety trade associations, federal user groups, as well as service providers, equipment vendors and other industry segments.

Waiver Order

- The Commission released a waiver order on May 12, 2010, granting 21 jurisdictions the ability to build an interoperable broadband network on 10 MHz of spectrum in the 700 MHz public safety band, subject to certain technical, operational and governance conditions.

➢Technical Conditions

- Common Air Interface using 3GPP Standard, Evolved Universal Terrestrial Radio Access (“E-UTRA”), Release 8 (“LTE”), and associated Evolved Packet Core (“EPC”).
- Coordination among Petitioners
- Out of Band Emissions
- Roaming (home-routed traffic, and local breakout traffic)
- Applications (Internet access, VPN access to any authorized site and to home networks, a status or information “homepage”, access to responders under the Incident Command System, and field-based server applications)
- System Characteristics, Interfaces and Testing (Interfaces, Interface Interoperability Testing (IOT), Devices, Standards Conformance Testing, Security)
- Governance and Coordination with the State
- Submission of Interoperability Plans to ERIC
- PSCR/DC Demonstration Network

Interoperability Showing

- As part of Waiver Order conditions, Waiver Recipients were going to demonstrate their detailed deployment plan and network compliance through a set of guidelines established by ERIC.

➢Interoperability Showing

- General Guidelines
- Interoperability Components
    - System Architecture (Radio Access Network (RAN) Architecture, Core Network Architecture, Interfaces, Mobility and Handoff (handover), Roaming, Priority Access and QoS, Security, Devices)
    - Applications
    - Reliability and Availability
    - Radio Frequency Engineering (Radio Access Network Planning, Interference Coordination)
    - Testing
    - Deployment
    - Operations, Administration and Maintenance (OA&M)

Towards Final Interoperability Rules

- Identify the Gap between current technical / operational requirements as set in the waiver order and the final rules to be set for ultimate interoperable networks.
- Fill the Gap Through
  - ERIC with its advisory committees
  - Work done by PSCR and experience gained through public safety demonstration network
  - Public Comments through NPRM process

➢ Open Items

- A nationwide architectural vision for network and interoperability
- Key LTE Interfaces
- Regional PS Network ID (PLMN ID)
- Priority Access Schemes for PS Networks
- Roaming Arrangement (Clearinghouse)
- Security
- Conformance Testing and IOT
- Network Interconnectivity
- Coverage, Capacity, Performance and Reliability
- Interference
- And more?

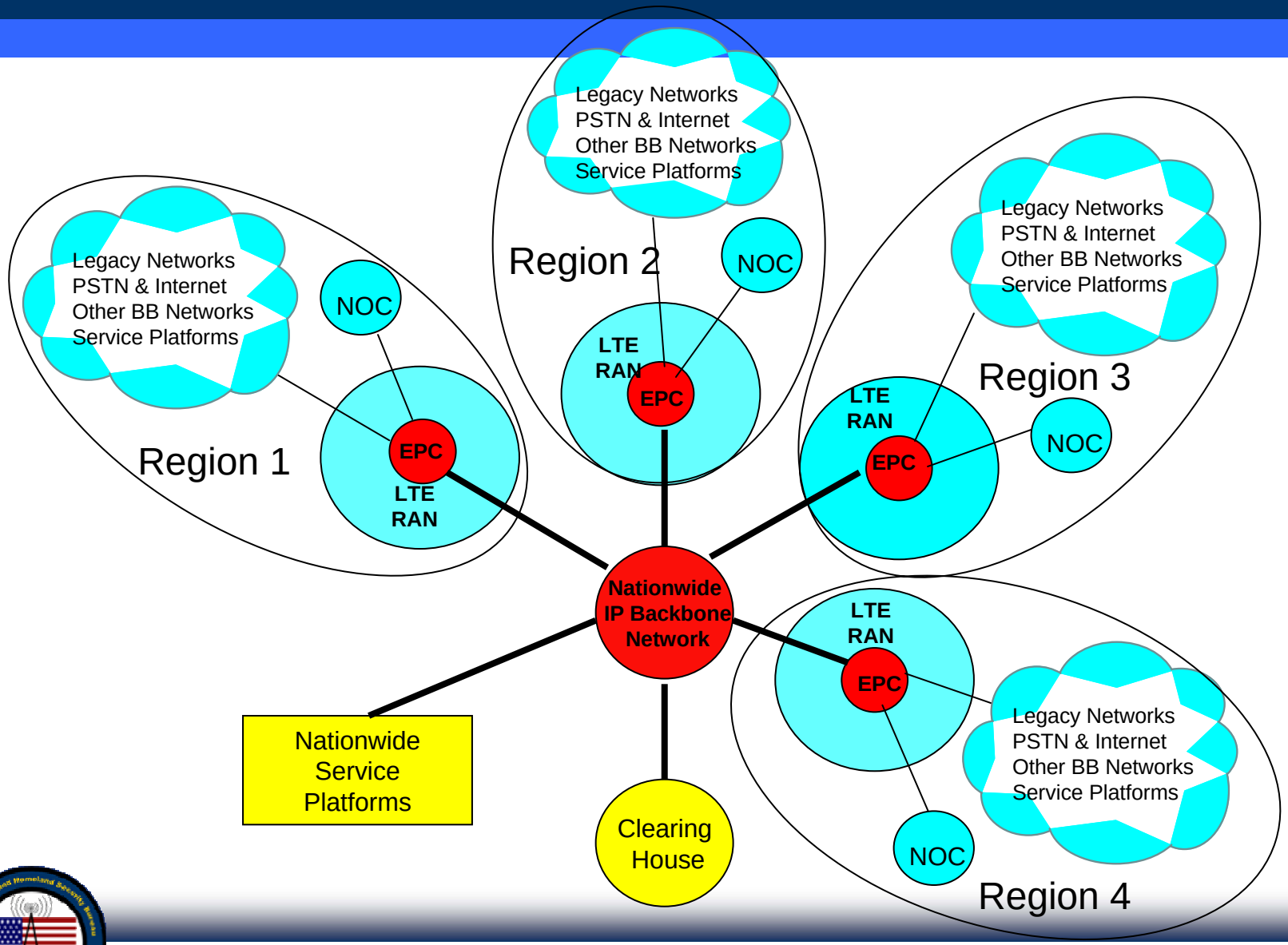
Architectural Framework

- The architecture of the public safety broadband network is critical to ensure nationwide interoperability.

➢ Architectural Guiding Principles

- Components of the Nationwide Network
- Regional Network Characteristics in support of
  - all-IP LTE technology platform (both E-UTRA and EPC) (3GPP at least R8)
  - commercial network technology with cellular network architecture
  - PLMN IDs scheme
  - key interfaces for interoperability as specified in LTE reference architecture
  - baseline applications
  - roaming capabilities such as Home-routed and Local-breakout
  - a nationwide framework for QoS and Priority Access
  - security schemes
  - a minimum level of spectrum efficiency
  - Coverage
  - a minimum level of coverage reliability
  - interference mitigation schemes
  - certain device capabilities
  - test verifications for interoperability (Conformance and IOT)
- Supporting Voice and Data Communications
- Roaming Authentication and Interworking Functions
- Nationwide Backbone Network
- Nationwide Services and Capabilities
- Evolution

Network of Network Architecture



Commercial Broadband Technology

- **Use improved commercial mobile broadband technology to meet and advance public safety mobile broadband service needs.**

- **Build a nationwide interoperable broadband network for public safety that**

- is designed based on proven **cellular architecture**,
- is based on advanced modern communications capabilities that continue to evolve,
- is feature rich by using feature capabilities of commercial networks,
- uses large and diverse eco-system of commercial devices and equipment,
- is based on commercial open standards,
- supports roaming and interoperability of commercial technology,
- supports mobility and seamless handoff of commercial technology,
- is efficiently managed and operated as commercial systems,
- has the option of using existing commercial network infrastructures,
- has improved performance and reliability that exceeds those of commercial networks,
- is cost effective as commercial networks are.

Cellular Architecture

➢ **Cellular architecture**

- is a well proven worldwide network design architecture that covers more than 5 billion subscribers worldwide,
- intertwined with commercial broadband technology, and hence, provides all the benefits – modern communications, feature rich, eco-system, open standards, roaming and interoperability, mobility and seamless handoff, huge commercial assets, and cost effectiveness.
- is supported by an array of well developed engineering design tools,
- provides operational efficiency due to economy of scale,
- provides flexible coverage and capacity with frequency reuse, and hence, spectrum efficiency.

LTE Technology Platform

- Overwhelming record support for LTE as the common air interface
- An important first building block for interoperability
- Adoption of LTE, specifically at least 3GPP Standard E-UTRA Release 8 and associated EPC, for all networks deployed in the 700 MHz public safety broadband spectrum
- The uniform deployment of Release 8 (or subsequent releases) is necessary to ensure backwards-compatibility.
- **Questions:**
  - Are there any additional capabilities to be considered within the LTE technology platform?
  - Any consideration of rules to ensure upgrade to newer releases of LTE on a timely basis?
  - What is the evolution of LTE and its forward and backward compatibility and interoperability across various releases for various applications.
  - Recognizing the current support for both IPv4 and IPv6 in LTE, what should be the evolution and migration path for IP versions in the networks?

PLMN ID Proposals

- Compliance with 3GPP standards requires the use of Public Land Mobile Network (PLMN) IDs.

- *NPSTC BBTF Report* identifies two alternatives
  - use of a single PLMN ID for the entire public safety network, or
  - use of a different PLMN ID for each regional network.

- The issues relating acquiring and assignment of PLMN IDs are being worked out.

- A number of parties propose a hybrid scheme in which one separate PLMN ID would be assigned to each regional network, and a single PLMN ID would be assigned for the overall nationwide network.

- **Questions:**

  - What are the benefits and disadvantages of a hybrid approach? Would the use of a single nationwide PLMN ID be adequate to support the envisioned “network of networks”?
  - What mechanism should be used to acquire and assign PLMN IDs for the public safety broadband network? – compliance with IOC process and minimize cost and burden on public safety operators

Key LTE Interfaces

- Consider key LTE interfaces that serve Roaming and Multi-vendor Interoperability

- Roaming interfaces
  - Uu- LTE air interface
  - S6a – Visited MME to Home HSS
  - S8 – Visited SGW to Home PGW
  - S9 – Visited PCRF to Home PCRF for dynamic policy arbitration

- Other interfaces
  - S10 – MME to MME support for Category 1 handover support
  - X2 – eNodeB to eNodeB
  - S1-u – between eNodeB and SGW
  - S1-MME – between eNodeB and MME
  - S5 – between SGW and PGW
  - S6a – between MME and HSS
  - S11 – between MME and SGW
  - SGi – between PGW and external PDN
  - Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules)
  - Rx – between PCRF and AF located in a PDN
  - Gy/Gz – offline/online charging interfaces

Baseline Applications

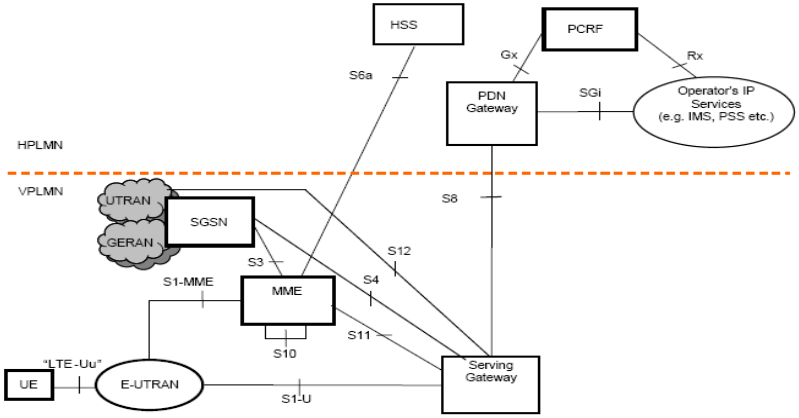
- To facilitate roaming, consider having access to a common set of applications – five required in waiver order as recommended in NPSTC BBTF recommendation
  - Internet access;
  - VPN access to any authorized site and to home networks;
  - a status or information “homepage;”
  - access to responders under the Incident Command System;
  - field-based server applications.

- **Questions:**

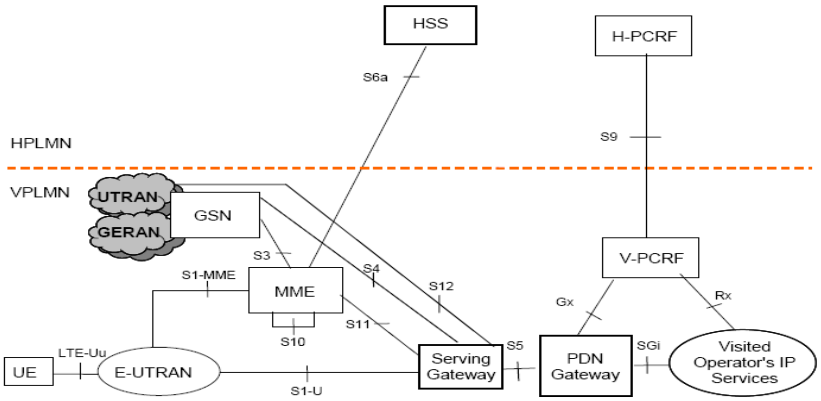
  - Would adding other applications contribution to nationwide interoperability? - The NPSTC BBTF Report recommends two other applications as “required” (1) Status/Information “SMS-MMS Messaging” and (2) LMR Gateway Devices. It also identifies four “desired” applications: (1) Location Based Data Capability; (2) One-to-Many Communications across all Media; (3) LMR Voice; and (4) PSTN Voice.
  - Are these applications capable of being supported at the present stage of technology and standards development? If not, when would they be ready?
  - Are there any other applications to be considered?

Roaming Configurations

- 3GPP LTE standards set two categories of roaming, home-routed and local breakout.
  - In home-routed, the roamer's traffic is routed back to the home network to enable the use of home resources
  - In local breakout, the roamer utilizes the resources of the host network for desired services.
- The Waiver Order required the support for both methods.
- Questions raised on these categories.



EPC Roaming architecture – Home routed traffic



EPC Roaming architecture – Local Breakout

Roaming Authentication & Interworking Functions

- Roamers need to be authenticated in the visited network as they would be in their own networks.
- Roaming authentication functions and any additional clearing functions between regional public safety networks require significant effort and resources to arrange, maintain and operate.
- Considering such functions to be performed by 3rd party clearing houses.

- **Questions:**
  - To what extent such clearing houses can perform the functions stated here?
  - Do they provide the performance, reliability and security that are required for public safety networks?
  - Is this solution cost effective?
  - Should there be a single third party clearing house, or multiple of them? If multiple, what is the right number?
  - Who should select the clearing houses, and what should be the selection criteria?

Interconnectivity

- Regional broadband networks will not serve as a nationwide interoperable broadband network unless they are interconnected.
- A number of solution alternatives for interconnectivity of regional broadband networks exist. A viable solution should have sufficient capacity (being fast), and be timely (low delay), reliable, secure and cost effective.
  - Direct interconnectivity
  - Internet
  - Third party operator's networks
- **Questions:**
  - Are there other solutions?
  - Which solution would provide sufficient capacity (being fast), and be timely (low delay), reliable, secure, scalable and cost effective.
  - If third party network is selected, should there be a single third party provider, or multiple of them? If multiple, what is the right number? Who should select the providers, and what should be the selection criteria?

QoS and Priority Access

- The broadband network needs to support prioritization among “connections” as well as “applications” - needs consistency in order to ensure nationwide interoperability.
- “Priority Access” is the network’s ability to determine which connections have priority over others in connecting to the network at times of emergency and network congestion.
- “QoS” is the network ability to assign classes to different applications based on certain performance attributes and objectives.
- “Priority Access” deals with the connection to the network while “QoS” deals with the treatment of traffic after the connection is established.
- During an emergency, network resources may be exhausted, and the Connection Admission Control has to reject new connections, preempt the existing connections, or lower their service priorities. This is when the Priority Access mechanism plays a role.

QoS and Priority Access – cont.

- Priority levels for connections can be defined and assigned based on various criteria including user's role (or user priority), user application types, incident type, etc.
- The determination of connection priority levels and its mapping to user priority, application type, and other attributes, is a matter that hinges upon both the public safety needs and the technology supporting it.
- LTE provides priority mechanisms through capabilities such as
  - "Allocation Retention Priority" (ARP) which assigns 15 levels of priority with two bits to flag preemption capability and vulnerability for a connection,
  - QoS Class Identifier (QCI) which assumes 9 levels of prioritization for various application types, and
  - "Access Class" barring that would allow any 14 levels of the access classes to be barred from the network at times of congestion.
- **Questions:**
  - Should we fully define a uniform priority scheme for all networks, or only some priority framework with flexibility for further refinement by localities?
  - Some questions on LTE capabilities - are they all fully available in 3GPP Release 8? Are they adequate to support a solid framework for priority access and interoperability?

Security

- Secure communications are of vital importance to public safety and will ensure interoperability by encouraging increased usage and reliance on the network.

- Security schemes are implemented at various levels and segments of the network to achieve an end to end reliable and secure communications. According to LTE specifications, five security feature groups are defined.
  - Network access security
  - Network domain security
  - User domain security
  - Application domain security
  - Visibility and configurability of security

- Each aspect of security as defined above is specified in various LTE standards.

Security – cont.

- NPSTC BBTF report required the optional security layer features specified in 3GPP TS 33.401 for network access security.
  - signaling layer security features over the Radio Resource Control (RRC) protocol layer (UE and eNodeB),
  - EPC signaling layer security features over the Network Access Stratum (NAS) protocol layer (UE and MME), and
  - user data/control layer security features over the Packet Data Convergence Sublayer (PDCP) protocol layer (UE and eNodeB).
- Considering to support both aspects of these security features, namely, “integrity protection and verification of data” and “ciphering/deciphering of data” be supported.
- **Questions:**
  - Are these the appropriate security features to ensure network access security for public safety broadband network?
  - Should rules be adopted for network domain security, user domain security, application domain security, and visibility and configurability of security? Would there be any interoperability issue, otherwise?
  - Does public safety require additional security? If so, what is it and what is the cost?

Conformance Testing

- Interoperability requires that user devices and network equipment comply with relevant standards specifications.
- Conformance testing, a process generally planned and developed by industry organizations and conducted by certified labs
- Conformance testing and certification process for user devices operating in LTE Band Class 14 is not ready yet.
- The PCS-Type Certification Review Board (PTCRB) is expected soon to complete development of such a process.
- **Questions:**
  - Do we need to require conformance testing and certification process such as PTCRB for devices?
  - Do the benefits of conformance testing outweigh the associated cost?
  - Questions on conformance testing for LTE infrastructure equipment.
  - Is there any known conformance testing with some formal certification process for LTE infrastructure equipment?

Interoperability Testing (IOT)

- Interoperability testing is an important mechanism for ensuring that public safety broadband networks are technically capable of supporting roaming.

- Roaming interfaces subject to IOT.
  - Uu – LTE air interface
  - S6a – Visited MME to Home HSS
  - S8 – Visited SGW to Home PGW
  - S9 – Visited PCRF to Home PCRF for dynamic policy arbitration

- Interim solution by network operators submitting IOT plans to Bureau

- Final solution through designating a lab for IOT

- **Questions:**

  - What are the costs and benefits of IOT on roaming interfaces?
  - Should there be IOT rules to ensure multi-vendor interoperability for public safety broadband networks?
  - What and how to designate a lab? Test plan? Cost?

Performance

- Public safety networks must meet baseline operability requirements including a baseline spectral efficiency, to insure interoperability.

- Achieving high spectral efficiency will enable the delivery of broadband services, and the universal availability and interoperability of anticipated applications, to the largest possible number of users.

- Consider providing outdoor coverage at certain minimum data rates at certain sector loading, for all types of devices, for a user at the cell edge.

- Consider requiring network operators to certify, within certain time of date of service availability, compliance to these data rates.

- **Questions:**

  - What would be the impact of not requiring such performance measures?
  - What would be the cost of supporting such performance measures?
  - What data rates should be adopted for UL/DL at the cell edge? Should they be minimum or average rates?
  - Should there be other mechanisms to insure spectral efficiency?

Coverage

- To ensure a baseline level of service and interoperability across the country, consider a certain level of coverage.

- **Questions:**
  - Population-based coverage or geographic coverage? Advantages and disadvantages?
  - What percentages either way? What timeframe?
  - Any interim benchmarks for the percentage of population or geographic area covered?

Coverage Reliability

- While coverage of a network is important to ensure a baseline of nationwide interoperability, coverage reliability (or signal reliability) is another critical factor.
- Areas of poor performance and inadequate coverage must be identified to ensure that a sufficient level of operability and interoperability is maintained throughout the network.
- Consider providing certain level of coverage reliability for all services and applications throughout the network.
- This requirement finds support in several of Petitioners' interoperability showings, and is a standard commonly used today by the Land Mobile Radio and Cellular industries.
- **Questions:**
  - Questions on imposing such requirements
  - What level of coverage availability?
  - What is the associated cost?

Interference Mitigation

- Considering the *Waiver Order* requirements on coordination for network operators whose jurisdictions border one another.

- Considering interference mitigation techniques that will avoid signal/spectral efficiency degradation within a region and between overlapping or adjacent regions.

- **Questions**:

  - Should there be rules for the coordination of network operators?
  - Should there be rules for the interference mitigation? What are the costs and benefits?
  - Should there be requirements for eNodeB features, such as Static Inter-cell Interference Coordination (ICIC) for interference mitigation?
  - Should there be a requirement for the eNodeB feature, Semi-static ICIC? What benefit Semi-static ICIC offer compared to Static ICIC?
  - How would compliance with these eNodeB feature requirements be determined?

Robustness & Hardening

- The overwhelming record indicates the importance of resiliency and reliability of public safety broadband network.

- The past record (partnership with D Block licensee) acknowledges public safety's need for sites equipped with generator and battery backup power. Consider an opportunity to refresh the record with additional comment on this issue.

- **Questions**:

  - Should there be rules for robustness and hardening? What should they be?
  - How many hours of back-up power to each eNodeB site is required? Should this number be less for sites located on building rooftops, apartments or similar structures?
  - How about other alternatives such as solar power, etc?
  - Should the back-up power requirement include other network equipment located at the Radio Access Network site location?
  - How would compliance with backup power requirement be determined? Should there be a requirement to file with the Commission for verification (*.e.g.,* self-certification, etc.)?