

## I. General

In the Interoperability Showing, Waiver Recipients must demonstrate sufficient technical and operational details on their build-out plans to achieve operability and interoperability. In preparing their Interoperability Showings, Waiver Recipients are expected to employ sound engineering principles and otherwise comply with the requirements of the *Waiver Order*. ERIC will analyze the viability of the Interoperability Showings and ensure they are consistent with the terms of the *Waiver Order* and achieve interoperability.

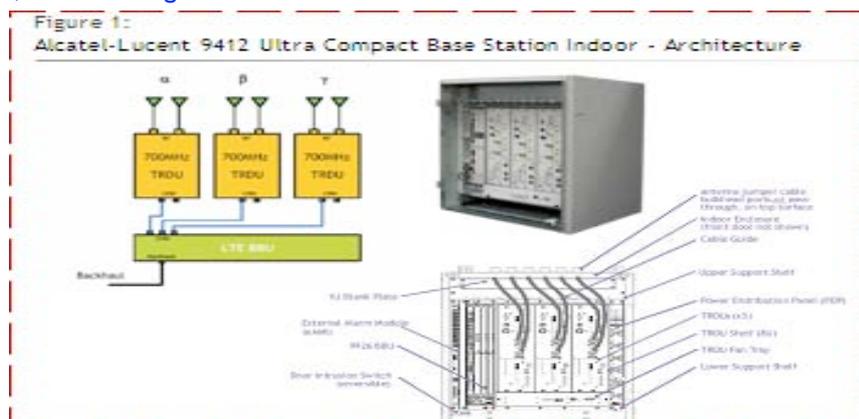
To facilitate the evaluation process, this Public Notice provides additional guidance to the Waiver Recipients for the purpose of the required Interoperability Showings. Adherence to this guidance is strongly encouraged to ensure uniformity in the filings, and a streamlined process both for the Waiver Recipients in preparing the showings and ERIC's review and analysis. Consequently, we request that the data submissions for the Interoperability Showings follow these guidelines:

- The Interoperability Showing should be prefaced by an executive summary of less than **5 pages**. This summary should provide a high-level explanation of how the Waiver Recipient's network will achieve interoperability.
- The Interoperability Showing should include sections addressing each interoperability component discussed in Section II below. We request that Waiver Recipients use Section II of this Public Notice as a framework for organizing the contents of their showings. Each showing must be less than **30 pages** (not including the executive summary) and in 11-pt. or larger type. Additional information can be submitted in appendices if needed; however, the content of the showing should be provided in the body of the document.
- All submissions should be in PDF format and all text should be searchable.
- Petitioners may be required to file non-standard sized documents in paper format.
- Waiver Recipients may arrange a brief Power Point presentation to ERIC highlighting the key elements of their showings. Presentations can be provided either in person or via teleconference. Contact Jennifer A. Manner at [jennifer.manner@fcc.gov](mailto:jennifer.manner@fcc.gov) or 202-418-3619, Public Safety and Homeland Security Bureau, to schedule a presentation.
- Interoperability Showings may be submitted under a request for confidential treatment pursuant to Section 0.459 of the Commission's rules.

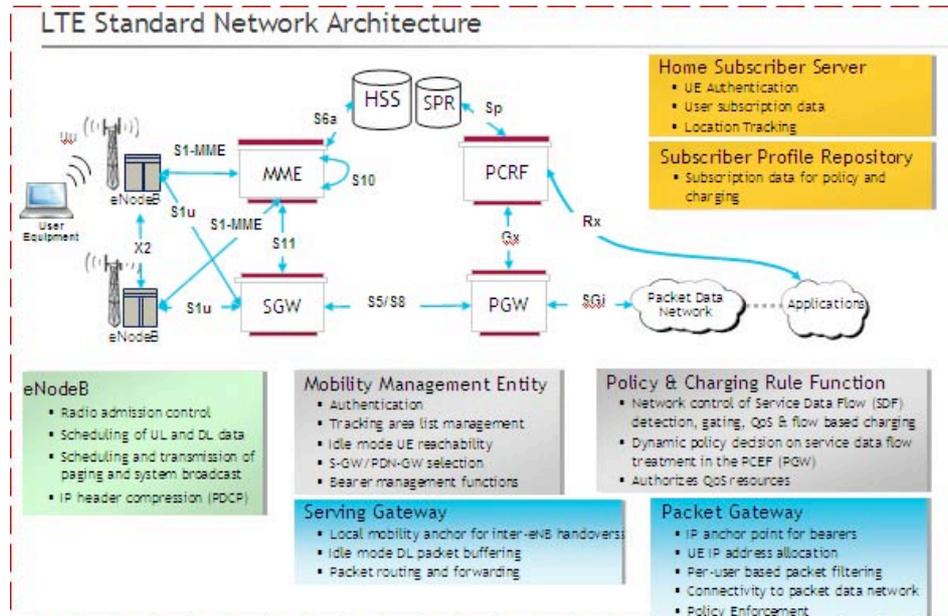
## Executive Summary

The City of Pembroke Pines proposes an LTE broadband network designed to meet interoperability goals of the City as well as adhering to the larger and long term goals of a nationwide public safety network. The proposed network will consist of LTE infrastructure components combined with a scalable, software-based, mobile communications middleware platform.

The infrastructure component is based on the Alcatel-Lucent 9412 enhanced Node B (eNB). The system offers extensive self-organizing network (SON) capabilities, leveraging open-standard interfaces between Alcatel-Lucent 9412 eNBs, to simplify operations and maintenance and make it easier to re-arrange networks when needed. The system makes use of preferred city sites and leverages, to the extent possible, the existing backhaul network.



Pembroke Pines will therefore be able to leverage the same authentication and mobility mechanisms used in commercial networks to enable seamless roaming across jurisdictions, as well as within commercial networks. The Home Subscriber Server (HSS) contains user information related to service provisioning, and LTE network elements use this information to handle calls or sessions, to locate and authorize users, whether they are roaming in home networks or visiting other networks. Specifics are covered in detail in Section II under Mobility Management Entity (MME). See Figure below:



The end-to-end solution will be compliant with 3GPP standards at all interfaces. Alcatel-Lucent's LTE solution uses standard 3GPP Release 8 procedures for mobility and handoff.

As specified in the waiver order, the suggested LTE solution supports two roaming architectures, home routed traffic and local breakout. Roaming using local breakout would allow services from the home network, the visited network, or a combination of the two.

Alcatel-Lucent's solution for Pembroke Pines supports the 3GPP policy and control architecture for determining QoS and Priority access for users and applications. At launch, the network will support all nine levels of QCI supported by 3GPP standards. Initial priority access capabilities will be introduced shortly thereafter and evolve over time along with standards

Security in the proposed LTE network will follow 3GPP recommendations, best industry practices, Alcatel-Lucent security requirements and other recognized security standards such as ANSI T1, Telcordia, CIS benchmarks, NIST and ITU X805. Thus a broad set of security features and capabilities is provided for the Pembroke Pines network. The authentication key agreement procedures which involve exchange between a UE and the LTE network will prevent rogue units from attaching to the network

Based on known LTE commercial device roadmaps and depending on the deployment window, a USB dongle, PC card or modem are the most likely form-factors anticipated at launch. Commercial public safety devices will likely support external antenna connections to enable the user of vehicle mount antennas to support improved performance. Soon thereafter, we also anticipate availability of

trunk mounted routers that would support a vehicle area network and potentially multiple wide area network (WAN) connectivity options.

Most commercial devices will have the capability to add specific clients for public safety operators when a new application server is developed to meet their needs. Alcatel-Lucent has committed to Pembroke Pines to work with their public safety organizations as well as other operators to develop or to partner on specific applications. As a suggested device specification, Pembroke Pines envisions minimum requirements for interoperability: laptop connectivity and vehicle solutions.

The Pembroke Pines LTE network will also be compatible with the following applications:

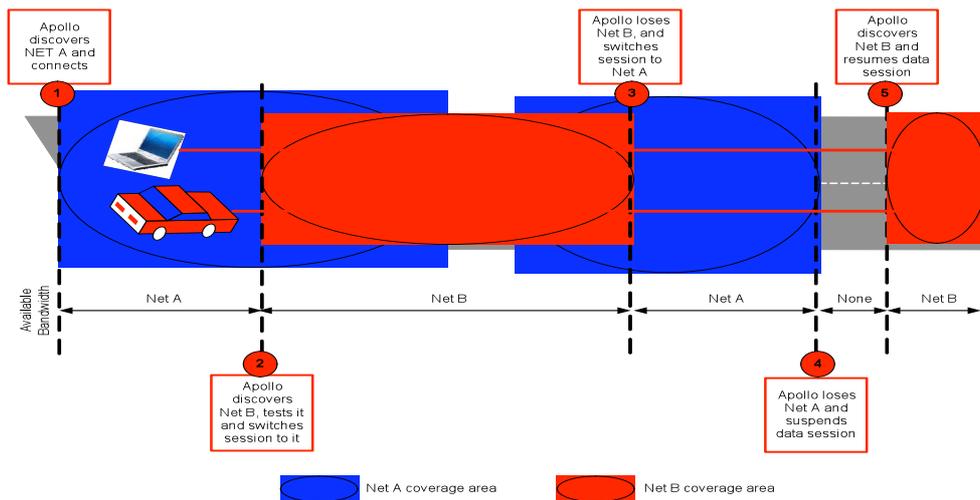
- Internet Access
- VPN
- Home Page
- Responders Under Incident Command
- Field Based Server Applications

The Radio Access Network sites will have on-site backup power of at least 8 hours for all of the network equipment. The system is designed with redundancy of the backhaul connection between an antenna site and the core infrastructure. The LTE network is designed with built-in high availability features to avoid any single point of failure

The City of Pembroke Pines will engage Alcatel-Lucent to Build, Operate and Transfer (BOT) the Pembroke Pines Broadband Public Safety LTE Network. In the build operate and transfer approach, Alcatel-Lucent builds the new network, operates and maintains the new network. At a pre-agreed timeframe, Alcatel-Lucent will begin to train City Public Safety personnel to efficiently operate the new network. Once Pembroke Pines personnel have been trained, all network operations activities are then transferred over to the City.

As an added enhancement to rapid interoperability capabilities, Pembroke Pines is also implementing the **Apollo Anywhere** platform. This solution has the unique ability to make multiple similar or dissimilar networks virtually appear as one – whether in a serial manner (true “make before break” seamless handoff of a secure data session across varied networks on hot standby) or in a parallel manner (actually taking multiple similar or dissimilar network connections – up to 20 – bonding them, aggregating their bandwidth, and using them simultaneously). This will enable interoperability with current and future networks – namely between the near term 700 MHz Public Safety Broadband Network, other private and commercial networks in Pembroke Pines and future Federal broadband networks.

Brand Communications’ Apollo Anywhere is a scalable, software-based, mobile communications middleware platform. It creates a virtual wide area network (VWAN) connection between remote devices and local area networks using secure Layer 2 VPN connectivity over one or multiple wide area communication channels. Apollo’s unique session management, seamless roaming and bandwidth aggregation features enhance the resilience and usability of communications over both mobile and fixed networks.



The Apollo Anywhere Platform has been developed and proven over 18 years in mission critical installations and is highly modular and scalable. Today it is the only commercially available product that has been used to provide make-before-break seamless handoff roaming of data between private 700 MHz systems and other dissimilar networks, including commercial wireless carriers. Any combination of wired or wireless networks is supported, including but not limited to:

- 700 MHz LTE-based public safety networks
- GSM/CDMA, GPRS, 3G HSPA and EVDO networks
- Wi-Fi – licensed or unlicensed
- WiMAX
- Satellite
- Cable, DSL and dial-up networking
- Ethernet and other LAN protocols

Pembroke Pines see the combined efficacy of its infrastructure and middleware solution make its public safety network proposal one of the strongest for scalability, versatility, and reliability.

## II. Interoperability Components

### A. System Architecture

A broadband LTE-based network consists of two parts, the Radio Access Network (RAN) and an Evolved Packet Core (EPC). There may be other core networks connected to the EPC that provide connectivity and packet transport for public safety services.

*Radio Access Network (RAN) Architecture.* Waiver Recipients should provide an architectural description and drawings of the RAN including functional descriptions and capabilities of each element. The RAN description and drawings should include all connections, clearly labeled, to include the backhaul configurations and connectivity to the core network. The architectural description should support the interoperability showing and reveal any issues that hinder interoperability.

The high level Radio Access Network architecture is shown in Figures 1 and 2, highlighting a base station equipped for 3 sectors and MIMO antenna technology, and leveraging a compact, yet highly functional aggregation router for interconnection with the backhaul network. The key elements of the Radio access network are described below:

- **eNB:** the eNB is the radio base station for LTE access. It supports the functions of radio admission control, scheduling of uplink and downlink data packets,

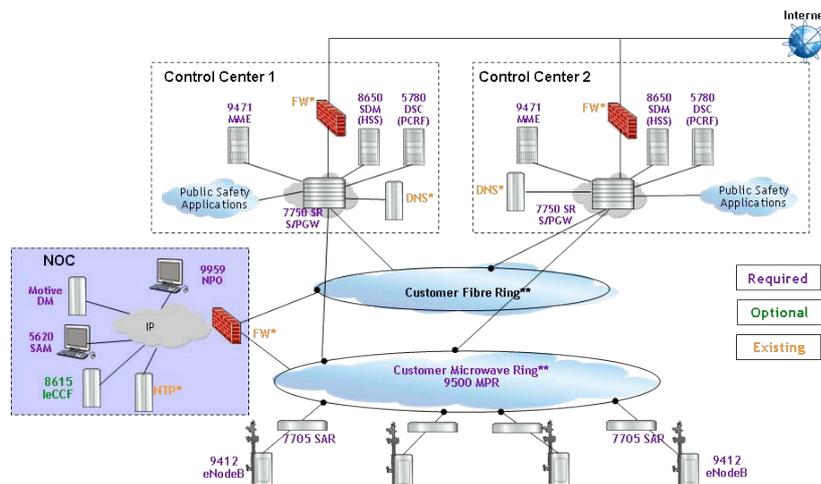
scheduling and transmission of paging and system broadcast, and IP header compression. The eNB product is the Alcatel-Lucent 9412 Ultra Compact Base Station, which comes in indoor and outdoor versions. It is optimized for 3 sector installations with MIMO in a compact cabinet.

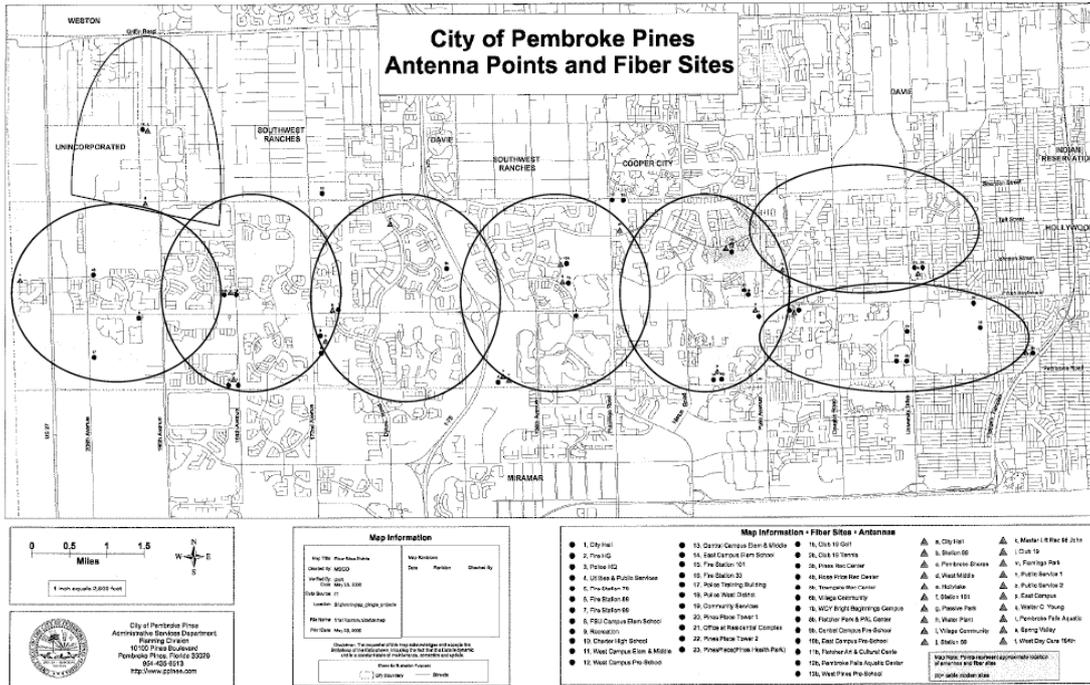
The indoor version (Figure 3) supports a baseband module which includes a controller module and up to three LTE modems, up to three radio/filter modules, or TRDUs (Transmit-Receive Duplexer Unit), which includes 3GPP band class 14 radios and filters in a single cabinet. The outdoor version (Figure 4) houses the baseband unit and backhaul aggregation router in one cabinet, and the TRDUs in a separate cabinet which can be located remote from the baseband cabinet with a CPRI (Common Public Radio Interface) standard fiber connection. 2x2 MIMO support is built into each TRDU (Figure 5).

The Band 14 TRDU is designed to support the full band 14 spectrum defined by 3GPP, and with software configuration will be capable of supporting RF configurations of 1 2x5 MHz carrier in PSBB block, 1 2x10 MHz carrier covering full band 14, or 2 2x5 MHz carriers, one each for PSBB and D block spectrum. As such, it is flexible to evolve in whichever direction the FCC regulations evolve relative to the D block, including future support for secure, segregated sharing of the eNB among a public safety operator and a commercial D block operator using the 3GPP MOCN (Multi-Operator Core Network) standards based methods.

- Backhaul base station router:** The Alcatel-Lucent solution supports redundant backhaul links at the eNB, using MPLS or routed connectivity. In some base stations, the connectivity is a direct fiber link using metro-Ethernet, in others it uses microwave point to point links. Both are connected to the eNB through an aggregation router. The Alcatel-Lucent product for this purpose is the 7705 SAR-8 (Figure 6). It is a highly flexible router supporting multiple backhaul link options, and enables backhaul link redundancy to meet the network resiliency requirements of public safety communications networks.
- Backhaul topology:** Definitive topology remains dependent on completed engineering surveys and studies. Below is a typical LTE Public Safety Network diagram and an overview of Pembroke Pines assets to be incorporated into the final design:

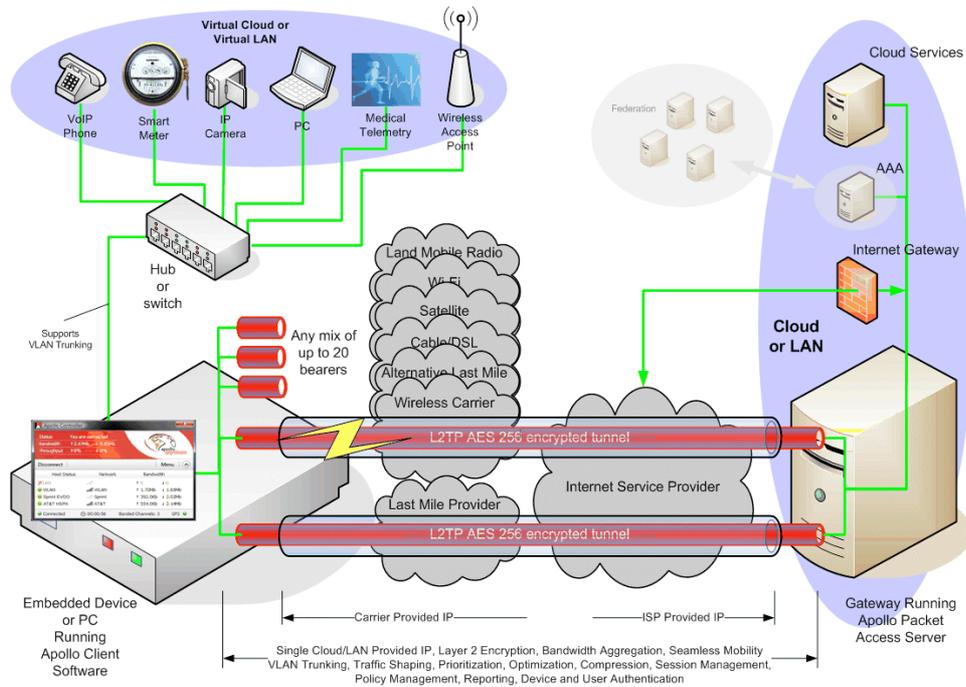
LTE Network Architecture for Public Safety





- **Backhaul aggregation router:** The core network router used is the 7750 SR, which is available in several configurations to support different aggregation points in the backhaul network for transport cost optimization. The 7750 SR is widely deployed in service provider networks globally, including wireline and wireless operators. As shown in Figure 8, it supports a wide range of networking protocols and is a highly available, carrier grade platform.

Apollo Anywhere Architecture



Apollo software clients are installed on remote devices (PCs, Smartphones, appliances/black boxes etc.). Apollo client then connects to Apollo Packet Access

Server installed on the edge of a LAN or Cloud platform. Client and Server establish an encrypted L2TP VPN tunnel over one or multiple simultaneous bearers and shapes, prioritizes and compresses traffic to boost performance. Client and server switch seamlessly between bearers and manage application persistence if connectivity is lost. Cloud VLAN architecture can be extended to edge devices across one or multiple simultaneous WANs; there are no Provider Provisioned services required. LAN/Cloud administrator remains in complete control of both ends.

*Core Network Architecture.* Waiver Recipients should provide an architectural description and drawings of the EPC and other core networks including functional descriptions and capabilities of each element. The Core Network architectural description should include all connections, clearly labeled, to include any interfaces planned for interconnection to non-LTE based or to commercial LTE network systems, if any. The architectural description should support the Interoperability Showing and identify any issues that hinder interoperability.

The high level architecture for the interoperable LTE network is shown in Figure 9, and 3GPP standard interface references are shown in Figure 10. Referencing Figure 10, the functional elements are mapped to the products included in PEMBROKE PINES's network in Figure 11. The end-to-end solution will be compliant with 3GPP standards at all interface, referencing Release 8 version of standards including December 2009 CRs for initial deployments. As standards evolve, the products will be software upgradeable to incorporate advanced functionality and future enhancements to the standards.

LTE roaming will follow today's GPRS roaming scenarios. Initially, security associations between LTE networks may be provisioned on a pair-wise, peer to peer relationship between operator network elements and interfaces to enable secure networking roaming. To scale to a larger, nationwide level, the pair-wise security associations must be avoided. To accomplish this, a border gateway between the network elements in each public safety operator's network will be required to securely connect roaming related network interfaces to a roaming exchange network (run by a 3rd party clearinghouse), enabling secure connections for roaming traffic to Mobility Management Entities (MMEs), Policy and Charging Rules Functions (PCRFs), Packet Data Network Gateways (PDN-GWs) and Home Subscriber Servers (HSSs) between visited and home networks. While this border gateway is not included in the initial network design, it will need to be added when public safety interoperability roaming requirements are finalized, and a clearinghouse chosen to broker the roaming relationships (See Security section for further information).

For the purposes of this interoperability showing, 3G interoperability with commercial operators is not described. However, Alcatel-Lucent supports an extensive feature set related to Inter-Radio-Access-Technology (Inter-RAT) roaming and handoff between LTE, HSPA, GPRS, as well as LTE and eHRPD. Voice interworking is also supported by the offering, including Circuit Switch Fallback (CSFB) as well as IMS VoIP Single Radio Voice Call Continuity (SR-VCC).

Description of the major network elements in the interoperable LTE network follows:

- **Mobility Management Entity (MME)** – The MME function in the LTE network is responsible for user equipment (UE) authentication, tracking area list management, idle mode UE reachability, S-GW/PDN-GW selection, and bearer management functions. The Alcatel-Lucent 9471 Mobility Management Entity serves this function in the network architecture (Figure 12). It is based on a high-availability ATCAv2 hardware platform, leveraging a redundant controller architecture and an extensive experience base in optimizing radio access

network and paging performance in wireless mobile networks.

The primary MME interfaces involved in interoperability among public safety networks and between public safety networks and commercial networks include the S6a interface to the HSS and the S10 interface between MMEs of adjacent operator networks. The S6a interface is critical to authentication of users, whether it be a home user or a roaming user. The MME must be able to communicate with other operator HSS's via the S6a interface to authenticate roaming users. This may be done through a direct association known to the MME, or securely via a 3<sup>rd</sup> party roaming clearing house.

- **Serving Gateway (S-GW)** – The SGW in the LTE network is responsible for local mobility anchor for inter-eNB handovers (using the S1 interface), idle mode downlink packet buffering, and packet routing and forwarding.

The primary S-GW interfaces involved in interoperability among public safety networks and between public safety networks and commercial networks include the S1u interface between the S-GW and the eNB for handoff between networks, and the S8 interface between a visited S-GW and the home PDN-GW.

- **Packet Data Network Gateway (PDN-GW)** – The PDN-GW in the LTE network serves as the IP anchor point for bearers, UE IP address allocation, per-user based packet filtering, connectivity to packet data network and policy enforcement. The PDN-GW can support many APN connections per gateway, thereby enabling different public safety entities to have secure connections to their own data centers without going through the public Internet. As the primary policy enforcement point in the LTE core network, it communicates with the PCRF to query for policy rules related to setting up bearer connections for users, for example whether to allow QoS, what kind of rate limits to enforce for particular users, and in the future, whether to provide one user priority treatment over another in a network congestion situation. It is responsible for tagging packets with associated QoS parameters, including DSCP, QCI and ARP parameters, to assure that the flows are treated appropriately from when they enter the network over the SGi interface all the way to the UE.

The primary PDN-GW interface involved in interoperability among public safety networks and between public safety networks and commercial networks is the S8 interface described above.

The Alcatel-Lucent S-GW and PDN-GW products are both based on the 7750 SR, the same platform that serves as the core aggregation router for backhaul (See Figures 13, 14). A new module, the Mobile Gateway Integrated Service Module (MG-ISM) is added to the 7750 chassis to enable the S-GW and PDN-GW functionality. The product allows both S-GW and PDN-GW functions to be consolidated on a single 7750 SR for Public Safety network configurations.

- **Policy and Charging Rules Function (PCRF)** – The PCRF is a rules repository and engine to enable network control of Service Data Flow (SDF) detection, gating, QoS & flow based charging at the PDN-Gateway. It enables dynamic policy decision on service data flow treatment in the PCEF (PGW), and authorizes QoS resources and priority treatment for users and applications. A summary of PCRF rules processing is shown in Figure 15.

The primary PCRF interface involved in interoperability among public safety networks and between public safety networks and commercial networks is the

S9 interface between the home PCRF and the visited PCRF. This interface allows a visited network to adjust policies to treat visiting users with a different grade of service than home users. This is important for public safety networks in that home users should typically have higher priority to access than visitors in an incident situation.

In the Alcatel-Lucent solution, the PCRF function is served by the 5780 Dynamic Service Controller (DSC). The 5780 DSC is a very flexible, high availability rules engine, and is available in two hardware configurations, a smaller Sun Server X4170 configuration and a larger ATCAv2 platform. Its architecture and network interfaces are shown in Figure 16.

- **Subscriber Profile Repository (SPR)** – The SPR is the 3GPP functional entity which stores the subscriber information which is related to Quality of Service and Charging details. 3GPP specifies the Sp interface to access the SPR data, but due to the large number of deployment variations, the specifications are not detailed, in comparison to other parts of the policy control and charging architecture. The 5780 DSC supports two modes of operations as described in Figure 17:
  - Collocated SPR – within the 5780
  - External SPR – in a separate database or collocated with the HSS

Alcatel-Lucent Public Safety deployments typically use the database in the HSS to store the SPR data.

- **Home Subscriber Server (HSS)** – The HSS is the 3GPP functional entity responsible for user equipment authentication, storage of user subscription data, and location tracking of the user. It is a fundamental roaming enabler in the LTE network. As mentioned above, the key interface interconnecting with the HSS for roaming is the S6a interface from the MME.

The Alcatel-Lucent LTE solution uses the 8650 SDM to provide both the HSS and the SPR functions (see Figures 18 and 19). It also is capable of providing a 3G HLR for both CDMA and GSM/UMTS networks, and so can be useful if the public safety operator desires ultimately to roam with 2G or 3G networks, especially for voice in the future.

*Interfaces.* Waiver Recipients should provide a list of interfaces that are in compliance with 3GPP Release 8 of the LTE standard, including those specified in the *Waiver Order*. They should also provide the list and description of those interfaces that are not fully compliant with 3GPP Release 8 of the LTE standard, with an analysis on the interoperability impact, if any.

Compliance statements below refer to 3GPP Release 8, with December 2009 CRs at initial network operation (compliance statements refer to Alcatel-Lucent Release LE3.0):

Interface	Description	Standards compliance
Uu	User equipment to eNB	compliant
X2	eNB to eNB	compliant
S1-u	eNB to SGW	compliant
S1-MME	eNB to MME	compliant
S5	S-GW to PDN-GW, home	compliant
S6a	MME to HSS	compliant
S8	SGW to PGW, roaming	compliant
S9	PCRF to PCRF, roaming	future compliant (2H2011 est)

S10	MME to MME	compliant
S11	MME to S-GW	compliant
Gx	PDN-GW to PCRF	compliant
Rx	Application Function to PCRF	compliant

*Mobility and Handoff (Handover).* Waiver Recipients should describe how nomadic, portable and high speed (75 mph) mobility and seamless handoffs are achieved according to 3GPP Release 8 of LTE specifications between base station nodes within the region's broadband network. Further, they should describe how the system provides mobility across base station nodes while maintaining a secure connection (VPN session) and session persistence in a portable environment. They should also describe how the system handles mobility and handoff when entering into adjacent regional public safety LTE networks. Waiver Recipients should also describe if any other handling features are provided, and if there is any interoperability issues.

Alcatel-Lucent's LTE solution uses standard 3GPP Release 8 procedures for mobility and handoff. Within the network, the solution supports both X2 and S1 handoff methods to assure uninterrupted connections when a user moves between eNBs. Handoff timing for these types of handoffs in a well engineered network expected to be between 50 and 100 milliseconds at time of launch, and will readily support mobility speeds of 75 mph. These handoffs are transparent to the user's IP address, which remains anchored at the PDN-GW for the duration of the user's data session. In this manner, secure VPN connections (e.g. IPsec VPN) will be uninterrupted as the user moves throughout the network, as long as a gap in LTE coverage does not exceed the VPN's timeout interval (typically more than 5 seconds).

When moving between adjacent networks where a different MME is involved, the S10 interface may be used to transfer user and session context parameters between networks, thereby accelerating the handoff and minimizing the time required to set up a bearer in the visited network on the new network's S-GW. It is also feasible, with appropriate internetwork security agreements, that the original network's S-GW can remain in the data session, if the visited eNB allows connectivity to the home S-GW. Such negotiated arrangements may be advisable when border handoffs are expected and can be involved in a mission critical situation, as may be the case when two large metropolitan areas are adjacent to one another across state borders (e.g. NYC and NJ). In either case, the home PDN-GW would remain in the call and the user's IP address would be maintained across handoff borders.

The Apollo Anywhere interoperability solution offers the flexibility to interconnect LTE and non-LTE based or commercial LTE network systems, in addition to any other wired, wireless and satellite data network. It provides full control of NIC and modem hardware allowing users to coordinate communications over multiple networks while dispensing with multiple connection managers. It also creates a true make-before-break seamless handoff between any wired or wireless networks that ensures no gaps in communications between the remote user (including nomadic, portable and high speed users) and the LAN platform.

*Roaming.* Waiver Recipients should provide a description of their roaming capability to and from other regional public safety broadband networks based on the requirements specified in the *Waiver Order*. Additionally, such description should include roaming to and from commercial networks, if provided. Responders should also provide operational plans concerning roaming, and specify their intent for roaming agreements with other jurisdictions, if any, until the FCC's final rules are in place.

In LTE networks the key identifier involved in network identification is called the PLMN ID (Public Land Mobile Network identifier). The PLMN ID is broadcast by the eNB to identify the network(s) that are available through that eNB. The PLMN ID is used by UE

in Idle mode for PLMN selection, cell selection/reselection. To support inter-PLMN cell reselection, the Equivalent PLMN list is used. The capability to allow or disallow roaming to specific PLMNs is based on the definition of a PLMN ID list which is programmed in the UE. Specific access restrictions can also be implemented based on PLMN ID, e.g. barring of certain outgoing call types when roaming outside of the home PLMN. PLMN ID may be used to identify the home network of visiting users for the purpose of aggregating roaming usage for accounting purposes

The user equipment (UE) is also associated with a home PLMN. The home PLMN ID of a UE is used to identify the HSS to retrieve subscription information by the visited network. Each UE has an associated IMSI, (International Mobile Subscription Identifier), a unique mobile number programmed into the device's SIM card. The PLMN ID contained within the IMSI is used by the MME to determine whether a visiting user is allowed to connect as a roaming user. It can also be used to identify visiting users and override the requested QoS and insure that home users receive higher priority and QoS treatment.

Alcatel-Lucent recommends limiting the total number of PLMN IDs associated with Public Safety networks in the US, in order to facilitate numbering plans and roaming. This recommendation is supported by the FCC's waiver order. It is recommended that in most cases that a PLMN ID be allocated on a statewide basis, with the exception of some major metropolitan areas like New York City or Los Angeles. In this manner, the total PLMN IDs associated with the interoperable broadband network can be limited to approximately 60, a manageable number. The implication of this is that a single PLMN ID corresponds to a single core network (EPC). Although the current plan for this waiver network is that a core network is included in the build out, it is our view that the core network PEMBROKE PINES deploys would serve neighboring regions to minimize these issues. Unfortunately BTOP funding did not permit this consideration. Alternatively, PEMBROKE PINES will investigate other core sharing options.

To enable seamless roaming, the UE must have an allowed list of PLMN ID's programmed into its SIM card. The number of entries in this list is limited in practice. To minimize UE complexity in this regard, Alcatel-Lucent proposes to use an umbrella Public Safety PLMN id that is used nationwide and broadcast from every Public Safety eNB in addition to the PLMN ID of the home network with which the eNB is associated. (HPLMN ID). There may or may not be any subscribers that have that nationwide PLMN id as their HPLMN. Each Public Safety eNB (PSBB spectrum) would broadcast two PLMN IDs in its SIB1 (System Information Block) message, the HPLMN id the eNB serves and the nationwide PLMN id. Note that the capability to broadcast multiple PLMN IDs will not be available at launch, but is expected to be available in 2H2011.

The allowed PLMN list, or "white list" in the UE would contain its HPLMN, the nationwide PLMN, and possibly a few commercial PLMNs, depending on spectrum band and technologies supported by the UE. It might include commercial network PLMN ids to allow roaming outside the PSBB network in the event that no PSBB spectrum coverage is present in an area. In this manner, UE roaming across the country could readily be supported, where each UE would include its own HPLMN id and the nationwide PLMN id in the white list, limiting how many PLMN ids a UE may have to know about. It also avoids the need to update the white list whenever a new PS PLMN is defined.

As specified in the waiver order, the suggested LTE solution supports two roaming architectures, home routed traffic (Figure 20) and local breakout (Figure 21). An example of home routed traffic would involve initiating the user's LTE network attachment by connecting to an APN (Access Point Name) in the user's home PDN GW

that supports connectivity to their home based applications. Roaming using local breakout would allow services from either the home network, the visited network, or a combination of the two. Example is an internet APN Architecture selected per APN. Some APNs associated with a user can be using home routed traffic, while others can use local breakout.

Apollo Anywhere supports VLAN, or multiple trunked VLANs, over wide area networks allowing all LAN topologies to be effectively extended over the wide area with session persistence during out of coverage situations. It provides resilience and recovery from lost connections using algorithms that manage application persistence at both client and LAN ends of wide area connections. Apollo features mobile-optimized VPN encryption with very low overhead ensuring optimal performance of VoIP and similar protocols over low bandwidth links or transparency to existing VPN encryption. There is complete transparency across wide area networks using Layer 2 tunneling that allows users to control and manage connectivity without relying on Provider Provisioned VPLS, MPLS or IP VPN services.

*Priority access and QoS.* Waiver Recipients should provide a description of priority access schemes and Quality of Service (QoS), if they are implementing and operating these capabilities in their networks. They need to discuss the impact of such implementation on the nationwide interoperability of the public safety network.

QoS and Priority Access with pre-emption are critical capabilities for the mission critical applications that are required by Public Safety. Some examples of key public safety applications requiring priority access and QoS include:

- Mission critical video, such as a helmet mounted camera on a first responder in a fire situation (requiring high priority video)
- Situational awareness such as used to identify a suspect in a crowd/terror situation (requiring high priority, and high resolution video (HD-quality))
- Remote control of robotics, as used to disarm a bomb (requiring high priority and very low latency)
- Mobile command center (requiring high priority, high bandwidth, and varied QoS streams)
- Push-to-talk (requiring high priority and low latency)
- Internet and database access (typically only need best effort data)

The Broadband Network must support the ability to prioritize users as well as applications. It should support multiple levels of priorities that can be separately assignable to individuals or applications. In addition, the prioritization scheme should allow for the following:

- Ensuring that critical users remain continuously connected even as many critical and non-critical users attempt to use the network and the network becomes saturated.
- Ensuring that critical users are able to newly connect to the network, regardless of use or saturation and even if non-critical users must be disconnected or limited.
- Providing sufficient priority mechanisms to key applications such as voice and video that would otherwise suffer in the event of interruption.
- Enabling critical users to remain connected as they roam from cell to cell.
- A prioritization scheme among the first responders, so that in the event of saturation by the first responders themselves, the incident commander can prioritize particular applications or particular groups of responders.

- Dynamically prioritize users and applications in a segmented area of the Network (i.e. in the case of a localized incident).
- Priorities must be maintained as roaming is allowed, and as users roam onto the nationwide SWBN

The Alcatel-Lucent solution supports the 3GPP policy and control architecture for determining QoS and Priority access for users and applications. In this architecture (Figure 22) the Application Function (AF) requesting QoS or priority access negotiates the appropriate bearer characteristics with the PCRF. The PCRF also checks with the Subscriber Profile Repository (SPR) to determine if a user is authorized for these capabilities. The PCRF then requests the PDN-GW (the policy enforcement point, PEP) to establish a bearer for the user with the appropriate QoS and ARP (allocation and retention priority) values as determined by the PCRF rules and the input data from the AF and the SPR. PCRF rules can vary based on the nature of the emergency as communicated by the AF (which may be an incident command center), whether a subscriber is a home user or a visitor, and the geographic area of the user, as well as numerous other factors.

At launch, the Alcatel-Lucent solution will support all nine levels of QCI supported by 3GPP standards (Figure 23). Initial priority access capabilities will be introduced shortly thereafter and evolve over time along with standards. For priority access Alcatel-Lucent is leveraging work done by the industry team working NGN GETS. They determined the potential congestion points in the LTE access and IMS core networks – and proposed mechanisms to provide priority service for particular groups of users. The potential congestion points take into account both access (i.e., control channels) and traffic (i.e., bearer channels). Those mechanisms include:

#### Air interface congestion control

- Access class barring can be used to ensure high priority users can attach to the network by blocking regular users during congestion periods, thus reducing access attempts by high priority mobile devices. Additionally, the “high priority” parameter in the establishment cause information element can be used when a mobile attempts to establish a connection and is proposed in paging cause when the network pages the mobile on behalf of a high priority user.
- Priority paging enables priority calls to be delivered more reliably when the air interface is experiencing congestion

#### eNodeB and Evolved Packet Core Elements (EPC)

- Use of allocation and retention priority (ARP) values when network elements are in a processor or other resource overload condition
- Use of Allocation and Retention Priority (ARP) values to prioritize radio bearer admission
- DSCP marking on packets, and P-bit on Ethernet frames

Apollo Anywhere provides QoS across all bearers. It provides traffic shaping and real-time prioritization through deep packet inspection that allows users to manage how applications, protocols and VLAN traffic have access to available bandwidth. It permits fixed or dynamic IP addressing to any client device over the dynamic address carrier network and without any enhanced services being required by the carrier. Apollo also provides Compression and optimization of traffic *before* encryption with AES 256 algorithms ensuring maximum performance across the wide area networks. One of the unique features of Apollo is bearer bonding that enables applications to address and consume the aggregate bandwidth of

multiple private and/or commercial networks without requiring pre-allocation of bandwidth – to ensure delivery of mission critical data.

*Security.* Waiver Recipients should provide detailed specification for the security features they intend to employ for their networks. This should include the selection of features from 3GPP Release 8 of LTE security features as specified in the *Waiver Order*. Various security features for Key Management, Encryption, Authentication, Authorization, and Identification should be demonstrated. Waiver Recipients should also demonstrate any interoperability issues that may arise from the selection of these security features.

Secure communications links are vital to the majority of public safety practitioners. Security mechanisms are a major component of commercial technologies and their standardization. The Broadband Network must allow highly secure public safety applications, including local, CLETS and NCIC database traffic the ability to securely traverse the network. The Network must support Virtual Private Networking (VPN) sessions administered by local jurisdictions.

Mutual authentication of network and user devices is a fundamental part of the LTE security architecture. Master keys used for ciphering are never transmitted over the air and random challenges are used. Security in the proposed LTE network will follow 3GPP recommendations, best industry practices, Alcatel-Lucent security requirements and other recognized security standards such as ANSI T1, Telcordia, CIS benchmarks, NIST and ITU X805. Thus a broad set of security features and capabilities is provided by Alcatel-Lucent’s LTE solution.

At the radio interface, both encryption and integrity protection are supported for Non-Access Stratum (NAS) and Access Stratum (AS) signaling traffic, as well as encryption of the user plane (UP) traffic. This is illustrated in the table below (per 3GPP 36.300-910).

Confidentiality Protection (Encryption)	Integrity Protection	
	NAS Signaling	Required and terminated in MME
U-Plane Data	Required and terminated in eNB	Not Required ( <i>Note 1</i> )
RRC Signaling (AS)	Required and terminated in eNB	Required and terminated in eNB
<i>Note 1:</i> Integrity protection for U-Plane is not required and thus is not supported between UE and Serving Gateway or for the transport of user plane data between eNB and Serving Gateway on S1 interface.		

The authentication key agreement procedures which involve exchange between a UE and the LTE network will prevent rogue units from attaching to the network and will ensure mutual authentication with top level keys only known to the HSS and the Universal Subscriber Identity Module (USIM). Alcatel-Lucent will support airlink encryption using AES or SNOW3 encryption algorithms at network launch, starting with 128 bit input keys. The following EPS algorithms have been defined, and use either 128 (or 256-bit input keys - future 3GPP item):

- NULL Algorithms (EEA0 for encryption and EEI0 for integrity)
- SNOW3G Algorithms (EEA1 for encryption and EEI1 for integrity)
- AES Algorithms (EEA2 for encryption and EEI2 for integrity)

*Note:*

- EEA0, 128-EEA1 and 128-EEA2 for both RRC signaling ciphering and UP ciphering are supported between the UE and eNB
- EEA0, 128-EEA1 and 128-EEA2 for NAS signaling ciphering are supported between the UE and MME
- All NAS signaling messages except those explicitly listed in TS 24.301 [9] as exceptions are integrity-protected between UE and MME
- All RRC signaling messages except those explicitly listed in TS 36.331 [21] as exceptions are integrity-protected between UE and eNB
- User plane packets between the eNB and the UE are not integrity protected
- EIA0 for Integrity is used ONLY for unauthenticated Emergency calls in limited service mode

Further, LTE architecture relies on 2 security layers. These layers provide a double protection for the access and core components of the network. For example, a successful intruder would need to compromise both security layers present in the access component and the core. The use of IP-Sec on the transport (backhaul) network will help mitigate the lack of security or confidence with a transport pipe from a 3rd-party provider. The protection of IP-based interfaces will be in accordance with 3GPP TS 33.210 and TS33.310 which define Network Domain Security. In particular, both X2 and S1 links can be optionally secured through an IPsec security framework with (security) associations terminating at a dedicated gateway on the edge of the EPC. A thorough description of related IP security services can be found in IETF RFC 2401 and 4303.

3GPP standards specify roaming interfaces for exchanging of operator's policies (S9 interface between Visited-PCRF and Home-PCRF), authentication exchanges (S6a interface of HSS), routing user-plane traffic to the HPLMN (S8 interface), or routing the user-plane traffic to the Visited PLMN for accessing local services or the Internet (SGi) (Figure 24).

Diameter interfaces exposed in roaming scenarios (S6a, S9) should be proxied to protect the backend network against various kinds of attacks that could affect their operation. Diameter proxy agents are used to forward Diameter traffic to another Diameter peer in order to handle the request. Proxy agents may modify packets and may originate rejection messages in case of policy violation, for example, in case of receiving requests from unknown PLMNs. In addition, a Universal Threat Manager (UTM)/Firewall may be deployed to protect the Diameter interfaces for additional security. Note that the GSMA specifications indicate that the GPRS Roaming Exchange/IP Exchange (GRX/IPX) is a trusted environment and therefore there is no need for additional security functions over and above those specified in GSM PRD IR.34. Therefore, the use of the UTM is optional.

Protection of the user-plane traffic (S8/SGi) has different considerations. The firewall/Universal Threat Manager function needs to consider the lack of security inherent in GTP. Specific security countermeasures to implement should include:

- **Ingress and egress packet filtering:** this will help prevent the PLMN from being used as source to attack other roaming partners.
- **Stateful GTP packet filtering:** only allow the traffic required, and only from the sources and destinations of trusted roaming partners. This will prevent other PLMNs from initiating many kinds of attacks. It will also prevent PDN-GW from having to process traffic from PLMNs that are not roaming partners as well as illegal or malformed traffic.
- **GTP traffic shaping:** in order to prevent DoS attacks directed against PDN-GW and shared resources of bandwidth from being consumed by an attacker or a subscriber, GTP rate-limiting should be implemented.

- **IPSec tunnels between partners:** due to the fact that GTP-U and the embedded user-plane PDUs are not encrypted, an attacker who has access to the data path (such as a malicious employee or hacker) who has compromised access can potentially capture a subscriber's data session. IPSec tunnels can be used as a countermeasure to such threats.

Apollo Anywhere provides mobile-optimized VPN encryption with very low overhead ensuring optimal performance of VoIP and similar protocols over low bandwidth links or transparency to existing VPN encryption. It features complete transparency across wide area networks using Layer 2 tunneling that allows users to control and manage connectivity without relying on Provider Provisioned VPLS, MPLS or IP VPN services. Apollo Integrates into a wide range of AAA platforms.

*Devices.* Waiver Recipients should provide specifications for their planned devices, including their type (form factor), operational specification, spectrum band coverage, future upgrades, and any additional information, if available. Waiver Recipients should address device interoperability concerns, if any.

To ensure the early availability of end-to-end LTE solutions, including the network and associated terminals, Alcatel-Lucent has developed strategic collaborations with various device companies. For widespread device development specifically targeted at the public safety community, it is critically important to leverage commercially available technology. Based on known LTE commercial device roadmaps and depending on the deployment window, a USB dongle, PC card or modem are the most likely form-factors anticipated at launch. Commercial public safety devices will likely support external antenna connections to enable the user of vehicle mount antennas to support improved performance. Soon thereafter, we also anticipate availability of trunk mounted routers that would support a vehicle area network and potentially multiple wide area network (WAN) connectivity options.

In the minimum configuration required for public safety, user devices will support the public safety broadband block and the upper 700 MHz D-block; that is, per 3GPP Band 14 operation. Some of Alcatel-Lucent's device partners are also envisioning additional 700 MHz bands, such as Band 13 and Band 17, to enable roaming with commercial operators, as well as EVDO and HSPA. Additional form factors like hand-held units and smart phones are also envisioned. However, commercialization plans for these multi-band, multi-mode devices and alternate form factors are yet to be announced by mobile vendors.

Most of these commercial devices will have the capability to add specific clients for public safety operators when a new application server is developed to meet their needs. Alcatel-Lucent will work with public safety operators to develop or to partner specific applications to support the needs of the first responders over the next-generation wireless infrastructure. As a suggested device specification, we would propose the minimum requirements for interoperability as follows:

### **Laptop Connectivity Solution**

#### Form Factor

- USB dongle or
- PCMCIA

#### Location

- Integrated GPS (NMEA data output)

#### Frequency Bands

- Band 14 (758MHz - 768MHz DL; 788MHz - 798MHz UL)
- Band 13 (776MHz - 787MHz UL; 746MHz - 757MHz DL)

- Band 17 (704MHz - 716MHz UL; 734MHz - 746MHz DL)
- FDD operation
- Support for 5 and 10MHz channel bandwidths
- MIMO Support

#### Protocols

- 3GPP LTE Release 8
- LTE device category 3 (minimum)

#### Transmit Power

- Transmit power 23dBm +/- 2dB for all 3GPP band classes

#### Host Software

- Connection manager
- Drivers for Windows XP, Vista, Windows 7
- Provisioning tool
- AT Command Set with Extended Functions

#### Certification

- Compliant with relevant FCC rules and regulations

#### Environmental

- Operating temperature range -20 ° to +55 °C
- Storage temperature range: -40 to + 85 °C

#### Interoperability

- LTE: multi-band product: bands 13,14, 17

#### Optional/Future Functionality

- Support for CDMA EVDO Rev A; 800MHz and 1900MHz
- Support for HSPA; 800MHz and 1900MHz

### **Vehicle Solution**

#### Form Factor:

- Ruggedized vehicle mount

#### Main features

- Broadband LTE Compliant with 3GPP Release 8 Specifications, upgradeable to release 9
- MIMO capability
- WLAN Connectivity
- Integrated GPS
- IP Router

#### Protocols

- LTE Compliant with 3GPP Release 8 Specifications, upgradeable to release 9
- LTE device category 3 (minimum)
- IP Router
- IEEE 802.3 Ethernet / IPv6/IPv4 Support
- DHCP server, NAT support

#### Frequency bands

- Band 14 (758MHz - 768MHz DL; 788MHz - 798MHz UDL)
- Band 13 (776MHz - 787MHz UL; 746MHz - 757MHz DL)
- Band 17 (704MHz - 716MHz UL; 734MHz - 746MHz DL)
- FDD operation
- Support of 5 and 10 MHz channel bandwidths

#### RF

- 2 Rx
- 1 Tx
- Transmit power 23dBm +/- 2dB for all 3GPP band classes

#### Interfaces

- LTE RF antennas access (primary antenna for Tx&Rx and secondary antenna for MIMO/diversity)
- GPS antenna
- WLAN antennas

- USB 2.0
- Ethernet (RJ45, including indicators)
- I/O Interface connector
- USIM slot
- Power input
- Power mains switch
- Indicator LEDs

#### Size

- Dimensions (mm) (Approximate): ~160 x 30 x 100

#### Environmental

- IP class IP 44
- Operating temperature range: -30 ° to +60 °C
- Storage temperature range: -40 to + 85 °C

#### Regulatory approval

- Compliance with the relevant FCC rules and regulations

#### Power Supply

- 10.6 – 16VDC, < 54 W maximum power

#### Security

- Ciphering, deciphering & integrity compliant with the 3GPP Rel 8.

#### Interoperability

- LTE: multi-band product: bands 13,14, 17

#### Optional/Future Functionality

- Support for CDMA EVDO Rev A; 800MHz and 1900MHz
- Support for HSPA; 800MHz and 1900MHz

The ability of Apollo Anywhere to connect via virtually any wireless or wire line protocol provides the widest range of device compatibility.

### **B. Applications**

Each Waiver Recipient's network will likely support a range of applications, including those required by the *Waiver Order*. The Waiver Recipient should describe in sufficient details how the applications required by the *Waiver Order* will be provided. The Waiver Recipient should also provide specifics on any additional applications to be supported on the network, and provide an assessment as to how such applications impact interoperability.

**Internet access** – Figure 25 shows a sample configuration required to support basic Internet access.

**VPN access** – Figure 26 shows a sample configuration required to support IPsec VPN access to the public safety entity's private network for end-to-end secure communications. In addition to this approach, the PDN gateway will support a secure APN connection to the agency's VPN if desired, which may be coupled with airlink encryption for secure connectivity without the enterprise firewall.

**Status information or home page** – This "home page" will facilitate access to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with visitors to the system (NPSTC BBTF Final Report, 9/2009). While several mechanisms are available to support this capability, such as http redirect to a captive portal as is used in hotel wifi networks, the requirements for this capability must be further defined to assure consistency of implementation across the nationwide footprint. Several factors must be addressed regarding definition of this capability to assure consistent behavior when a user is roaming, including:

- Does a user automatically get sent to their home PDN-GW when registering on the network, or is a local breakout roaming capability employed to direct them to the visited PDN-GW?

- Is the local entity permitted to provide any override controls to limit access to visiting users? Does the home page need to include some policy management controls, forcing the user to register before getting connectivity access, or is it purely for information purposes?
- Is this web portal page linked to the incident command system? For example, does an incident commander have the ability to authorize or deny specific users and adapt their priority level?

**Access to responders under the incident command system** – This capability will be available in a basic form at system launch using best effort data in either a secure manner (see Figure 26 using VPN connectivity) or an open manner (see Figure 25 as in Internet access) which is not advisable when secure communications may be required. As the applications evolve to support QoS and priority access to users and applications, they must integrate the capabilities required to interface to the LTE access network through the Rx interface for policy control of QoS and priority access. There may also be implications related to the visitor portal as indicated above.

**Field based server applications** - This capability will be available in a basic form at system launch using best effort data in either a secure manner (see Figure 26 using VPN connectivity) or an open manner (see Figure 25 as in Internet access) which is not advisable when secure communications may be required. Depending on the nature of the application, best effort data access to it may not be sufficient. If it is an important application server it should be configured as a priority user, and since it will be functioning as an application server it most likely should be authorized for maximum bit rate allowable by the system to support incoming data traffic from multiple public safety users.

The versatility of Apollo Anywhere to connect via virtually any wireless or wire line protocol gives the network the broadest possible range of applications scenarios, including, but not limited to those specified in the *Waiver*:

- Internet Access
- VPN Acces
- Status/Home Page
- Access to Responders Under the Incident Command System
- Field Based Server Applications

**C. Reliability and Availability**

Waiver Recipients should provide their plans for the reliability and availability of their network. For example, Waiver Recipients should discuss how the major elements of the system are highly available and/or redundant. This should include power systems, backhaul, site equipment, core network equipment and network operations centers (NOCs). The availability of radio signal within the service area, and any mechanisms that will provide redundant coverage (i.e., in the case of a base station outage) should also be discussed. Waiver Recipients should discuss the mean time between failures for all system elements, including devices.

The Radio Access Network sites will have on-site backup power of at least 8 hours for all of the network equipment. The system is designed with redundancy of the backhaul connection between an antenna site and the core infrastructure. The LTE network is designed with built-in high availability features to avoid any single point of failure and to provide resiliency and self-healing at various levels of the network. The following table shows the redundancy capabilities available for each of the key network nodes:

Network Element	System Redundancy	Geo-Redundancy or Geo-Diversity
-----------------	-------------------	---------------------------------

eNB	Modem redundancy (future)	N/A
MME	1+1 Blade Redundancy	Pooling (MME-1, MME -2, ...)
SGW	1+1 Blade Redundancy	Pooling (SGW-1, SGW-2, ...)
PGW	1+1 Blade Redundancy	1:1 Inter-chassis Hot Redundancy (PGW-1 + PGW-2)
Compact HSS	1+1/N+N Redundancy for different component	Act-Stby
PCRF	1+1 Blade Redundancy (ATCA)	Geo-redundancy (PCRF-1 + PCRF-2)

At launch there is no *automatic* mechanism for redundant coverage of radio base stations in the event of a failure, although some limited service might be available in parts of the original cell footprint. Given that LTE uses a frequency reuse pattern of one, the network uses power control to control the coverage area of a cell site. For future releases, Alcatel-Lucent is investigating software enhancements to leverage Self Optimizing Network technology to enable a public safety network to rapidly adjust coverage automatically to compensate in the event of the loss of an individual eNB. Rapid deployable cell on wheels may also be used to address the situation in the near term.

#### D. Radio Frequency (RF) Engineering

##### 1. Radio access network planning

Waiver Recipients should provide their proposed RF design guidelines and demonstrate how these guidelines and RF system implementation would meet their coverage and capacity needs. The showing should include link level analysis for the intended mobility scenarios and relevant applications, the initial planned sites, site configuration, channel bandwidth and reuse factors.

Please note that throughout the text *downlink* means outbound transmission from the radio site and *uplink* represents inbound transmission from the mobile/portable.

##### Inputs and Assumptions

The RF design is based on inputs provided by PEMBROKE PINES. When inputs were not provided, assumptions based on Alcatel-Lucent's RF experience are used to develop the design. If these assumptions are incorrect, then the potential impact could be an increase or decrease in cell count to achieve the required coverage. The geographic contour of PEMBROKE PINES's SERVICE AREA constitutes the target service area.

The following inputs and assumptions were considered:

- List of cell site locations provided including lat/long and antenna height information (if available)
  - If the design requires sites that are not included in the Pembroke Pines list we temporarily select sites from the FCC ULS database of towers and licensees
- GIS terrain and clutter database
- Coverage boundaries based on county boundaries
- Morphology boundaries based on available digital clutter data
- Radio sites assumptions are based on engineering specifications
  - Antenna Gain: While Alcatel-Lucent can provide 700 MHz sector panel antennas with up to 17 dBi gain, it is possible that zoning, or the building environment, may restrict the size, and directivity, of antennas to be used which could result in an increase in cell count. This design

- exercise assumes either 14 dBi or 16 dBi gain antennas with a 65° horizontal beamwidth
  - Cable and Connector Losses
    - Dense Urban/Urban: 2 dB
    - Suburban/Rural: 2.5 dB
  - eNodeB Transmit Power: 20W (43dBm)
  - eNodeB Noise Figure: 3 dB
- UE Assumptions are also based on Alcatel-Lucent experience with 700 MHz devices
  - UE Power: 200mW (23dBm). This figure is for the most part based on UE Category 3 as defined in 3GPP specifications. While it is possible to design for higher power levels, there will be a need to assess the amount of out-of-band emissions and whether a balanced coverage is maintained.
  - If this particular design calls for a vehicular rooftop antenna we choose a compact 5 dBi antenna, which when combined with about 3 dB cable/connector loss yield a UE EIRP of 25 dBm, i.e. 2 dB higher than for out typical commercial networks design.
  - If the design calls for in-building service we account for building penetration losses and portable loss if the device is assumed being carried by first responders
  - UE Noise Figure: 7 dB
- In most cases, such as trunk-mounted antennas or in-car UE, antenna height was assumed to be 1 m AGL. This assumption may change once Alcatel-Lucent has better knowledge of the operational environment. For example, a UE in a police car may be located at ~1m AGL while it can be close to 1.5 or more in a fire truck. For the same coverage an increase in the UE height will result in a decrease in the cell count.
  - When available, antenna heights listed in the Pembroke Pines's list are used noting that such heights are estimates only. If the available heights during actual deployments are found to be lower, the coverage based cell count can increase.
  - More importantly, the design will try to focus on antennas heights that are of about similar heights so not to induce too much overlap between radio sites footprints. In particular, when mixing tall sites and low sites in close proximity can result in bad downlink performance
- Frequency: 763-768/793-798 MHz which represents the PSBB block. A frequency reuse of 1 is used throughout the service area.
- Multipath channel model
  - Dense Urban/Urban: VehA 50 – 120 km/h
  - Suburban/Rural: VehA 50 – 120 km/h
- Uplink Cell Edge Target Rate: 256/512/768/1000 kbps depending on Pembroke Pines's requirement
- Probability of Coverage: 95%

Further, since Multiple Input Multiple Output (MIMO) processing is embedded in the base station and expected in the UE, antennas at radio sites are essentially of a cross-polar type to alleviate the poor spatial diversity gain that could be achieved in the 700 MHz band. Therefore, coverage and capacity calculations assume MIMO in a 2x2 configuration, i.e. with 2 antennas (in a single package) per sector at the radio site and 2 antennas in the UE. In the UE case only one antenna will be used for inbound transmission.

#### Link Budget

A link budget is required based on the inputs and assumptions provided above in order to estimate the cell count and ensure the proposed RF design meets the

specified coverage requirements. The design for a particular edge rate across all environments assumed that at a minimum a certain set of applications needs to be supported when the UE is at the edge of the service area or a cell footprint. Designing for lower edge rates would result in a reduction cell count.

### Cell Planning

Cell planning was accomplished with Alcatel-Lucent's RF planning tool, which accounts for link budget figures, digitized terrain and clutter data, is used to assess the amount of coverage footprint and provide an estimate of the cell count. A listing of the cell sites selected for the network and associated coverage plots are included in the Figures 27 through 29.

## **2. Interference Coordination**

Waiver Recipients should provide their proposed plan for interference mitigation techniques within the region and with adjacent regions, which will promote interoperability by minimizing radio frequency interference between them. They should describe how these techniques will be implemented within the network infrastructure and/or equipment.

In an LTE network, since radio resources used in a particular cell footprint are orthogonal both in time and frequency domains inter-cell interference is practically not a concern. LTE utilizes a frequency reuse of one, meaning the same carrier frequency is used across all cells. This is in contrast with typical LMR systems which require an extensive radio frequency planning exercise. In a frequency reuse of one system there is a potential for (co-channel) interference in the overlap region of two or more neighboring radio sites. This leads to degradation in user throughput. Mitigating such interference for operation, both within a given network as well as at the boundary of two distinct networks (whether using the same infrastructure vendor or not) can rely on a number of approaches which are defined in the LTE standard.

Techniques for mitigating interference in an LTE network are described in 3GPP 36.211, 36.901, 36.300 and 36.423. They can be broadly classified into the following four types:

1. Interference randomization
  - Frequency selective scheduling
  - Frequency hopping
2. Interference control
  - Uplink power control
  - Interference over Thermal (IoT) control in the uplink
3. Interference cancellation
  - Coding and signal processing at the transmitter or receiver
4. Inter-Cell Interference Coordination/shaping (ICIC)
  - Coordinated intelligent resource allocation

For same-vendor, intra-network interference management, the above mentioned techniques can be used to reduce inter-cell interference from neighboring cells. In addition, the use of block error rate (BLER) control and choice of suitable hybrid automatic request (HARQ) operating point can be used to further improve performance.

Further, as reflected by the various waivers submitted to the FCC in a number of regions, some of the neighboring jurisdictions are required to ensure operation at the edge of their service-area footprint. For interference management at the boundary of another vendor's network or at the boundary of two distinct networks, the above mentioned techniques, with the exception of ICIC, can be used because these techniques do not need to be coordinated across different cells. Since ICIC is an

optional feature in the 3GPP Standard, it requires both vendors to implement similar ICIC algorithms and exchange information. There is effectively no overall gain if ICIC is deployed by one network and not in the other. For example if “coverage area 1” has ICIC deployed with vendor A but the neighboring “coverage area 2” has deployed with vendor B without ICIC, coverage area 1 users will not see any improved performance. Moreover, coordination rules that will apply to neighboring regions would not be different from those used in commercial deployments, e.g. a power flux density limit could be mandated by the FCC.

Key differentiators of the Alcatel-Lucent solution are:

- The integration and interaction of ICIC with other RRM (radio resources management) functionalities, including scheduler and other interference management functionalities, to maximize the effect of interference reduction, while minimizing the complexity.
- The possibility to combine Inter-eNB collaborative ICIC with Self-Optimizing Network (SON), which exploits OPEX gains provided by SON and avoids manual and complex frequency/resource planning.
- The mixed use of proprietary and standardized indicators on X2 interfaces between eNBs which maximize the gain obtained by the Inter-eNB collaborative solutions.
- Alcatel-Lucent Bell Labs continuous innovation, reflected in the on-going studies and proposals for advanced fully-adaptive ICIC techniques to be introduced later.

#### **E. Testing**

Waiver Recipients should provide their initial and long term plans for testing of their system, including timelines, type of testing, network elements, devices and applications that are subject to testing, and test-bed. This showing should specifically show a plan for meeting the requirement of the *Waiver Order* that Waiver Recipients participate in the PSCR/DC demonstration network. Waiver Recipients should also address Standards Conformance Testing, and Interoperability Testing (IOT). Additionally, they should address issues that they may be facing, and potential problems that may hinder interoperability. All timelines or schedules should be in Gantt chart format.

Alcatel-Lucent employs a comprehensive testing strategy based on a proven hierarchical model to deliver both best in class quality as well as quick time to market. The availability of products covering the full network, from RAN to transport to Core to IMS and applications, as well as device partnerships, and robust lab environments replicating complete operator network, allows Alcatel-Lucent to validate the LTE Solution as it would be when deployed in the field.

The testing suite as illustrated in Figure 30 is composed of Network Element Test (NET), Cluster Level Test (CLT), Network Level Test (NLT), and Performance Assurance (PA). NET, CLT, and NLT are serial (with some overlap), with NLT being the final testing stage prior to a First Office Application (FOA) commercial deployment in a live operator network. PA begins in parallel with CLT and continuing through FOA.

- Network Element Testing
  - Feature Functionality and Requirements Verification of SW/HW of individual network elements
  - Platform integration, vendor management, HW certification
- Cluster Level Testing
  - Integration, verification/validation at sub-network level
  - RAN cluster: eNB integration, System Integration, System Validation

- Network Level Testing
  - End to End (E2E) Solution Integration and Validation
  - Pembroke Pines operations and end user scenario testing
  - Solution Capacity, Performance, Resiliency (CPR)
- Performance Assurance and Offer Support
  - E2E Voice/Data Quality and Applications Performance
  - E2E KPI Validation incl mobility and OTA performance
  - Transport design, validation and performance

In addition to Alcatel-Lucent's internal testing and validation processes, they are an active participant in the PSCR demonstration network, and anticipates tests to begin on band 14 eNBs in the Boulder network starting in October, 2010. They are working closely with the PSCR team to assure that the interoperability specifications defined for the PSBB network are sufficient to assure the goals of the network with respect to multi-vendor support, roaming, and choice of user equipment.

Alcatel-Lucent supports interoperability testing based per operator request, and recommends that such testing be executed per the well-established process of the Network Vendor Interoperability Testing (NVIOT) Forum to minimize operator effort and reduce testing intervals (See Figure 31). The NVIOT Forum is an organization of wireless network equipment vendors created to address the industry's challenges of assuring open interfaces and interoperability and reducing the interval required to deploy high-quality multi-vendor networks. The Forum accomplishes this by documenting best-practice testing methods, by authoring generic Master Test Catalogs (MTCs) for network interfaces which are quickly adaptable to specific IOT requests, by providing a template for interoperability testing engagements (from planning through execution, issue resolution, and documentation) that allows re-use of testing results across multiple operator requests, and establishing a basis of agreement between vendors which minimizes effort required by operators to drive vendor coordination. The Forum works in cooperation with standards bodies to address any standards errors or ambiguities found during testing.

The NVIOT Forum was founded in March 2000 by Alcatel, Lucent Technologies, Ericsson, Motorola, Nokia, Nortel Networks and Siemens and has expanded to include most other major infrastructure vendors. The Forum has facilitated interoperability for GSM and WCDMA and its charter was expanded to include the LTE/SAE technologies in May 2008. Specification of MTCs for 3GPP R8 based interfaces, which include those for LTE, in Q2 2008 and continues to develop Catalogs for LTE interfaces based on operator priorities represented by NVIOT Forum members.

Pembroke Pines will require all devices to successfully complete interoperability testing with all network infrastructure vendors included in Pembroke Pines' network, based on test plans provided by each network infrastructure vendor. In addition, Pembroke Pines will require all devices to complete any interoperability/certification testing as required by Pembroke Pines network roaming partners.

## **F. Deployment**

Waiver Recipients should provide a deployment plan that is sufficiently detailed, including milestones. This plan should include a timeline presenting phases of deployment as well as various stages of deployment within a phase such as site planning, network design, testing and trials, and operations. This plan should include the geographic coverage, the number of cell sites, and the technical/operational specifics on the potential partnership with other network providers, if any. Critical paths and milestones should be clearly designated. All timelines or schedules should be in Gantt chart format.

Network outsourcing is a strategic business and technology relationship between Alcatel-Lucent and Pembroke Pines to seek seamless operation of the existing legacy network, construction of new technology networks and migration to next-generation network architectures. Alcatel-Lucent focuses on the transfer of existing end-to-end network operation processes and related organizations, improving the efficiency of both while providing ongoing network operations services.

Pembroke Pines will engage Alcatel-Lucent to Build, Operate and Transfer (BOT) Pembroke Pines' Broadband Public Safety LTE Network. In the build operate and transfer approach, Alcatel-Lucent builds the new network, operates and maintains the new network. At a pre-agreed timeframe, Alcatel-Lucent will begin to train Pembroke Pines personnel to efficiently operate the new network. Once Pembroke Pines personnel have been trained, all network operations activities are then transferred over to Pembroke Pines.

Alcatel-Lucent's BOT services model provides clients with a complete set of services to prepare, operate, and assume ownership of a new LTE network deployment. These services include three primary areas:

- **Planning/Implementation:** Development of methods and procedures, and implementation of the platforms, people, and assets required to operate the new environment. Within this context, this is known as the "build" of the BOT operational model.
- **Operational Execution:** Operational support for all in-scope services which are measured and reported against the service level requirements. The Alcatel-Lucent team performs against agreed upon operational service levels. Their team and related knowledge begins to prepare for the transition back to the Pembroke Pines.
- **Transfer:** In this phase Alcatel-Lucent executes a transition plan to migrate the ownership of work back to Pembroke Pines. This includes the necessary people, processes, and assets. Through Alcatel-Lucent Services' proven processes, tools, methodologies and shadow-management training, a smooth operational transition can be designed for Pembroke Pines to mitigate risks in assuming the operational management of the LTE Network.

If Pembroke Pines will be purchasing and deploying some or all of their network elements, Alcatel-Lucent services will work with Pembroke Pines to determine an appropriate deployment schedule to meet their needs. A representative timeline is shown in Figure 32 outlining a deployment plan to build, test, integrate, and manage Pembroke Pines' broadband data solution. Alcatel-Lucent will deliver a high quality, fully functional, turnkey solution as well as user and operations level training. As a key system integrator, Alcatel-Lucent will have the responsibility for planning and end-to-end design, technical specification development, selection of products and platforms, deployment, installation, network integration, training and operational and maintenance support. As part of this process Alcatel-Lucent will define detailed project milestones, responsibility matrices, scope of work and deliverables. Key components to Alcatel-Lucent's program management office (PMO) would include:

- **Plan of record:** Plan of record (POR) will be developed to formally document all roles, tasks, dependencies, and activities required. The POR will be the governing document throughout the project.
- **Change management:** Based on the plan of record, the PMO will coordinate formal change management as required to ensure successful delivery.
- **Risk management:** The PMO will identify, analyze, and control risks in the project, build and execute mitigation plans as necessary, and report and escalate risks as required.

- **Communications management:** The PMO will adhere to the communications plan contained in the POR, and ensure efficient and timely communications including regular reporting of status, risk registers, and project health dashboards.
- **Material management:** The project management team will coordinate the definition of a detailed bill of materials and track the procurement and delivery of materials required to implement the solution for all vendors.
- **Third-party management:** The PMO will manage all vendors and partners participating in the project as defined by the POR.
- **Integration:** PMO will oversee integration activities with other relevant agencies and coordinate inter-agency operations.

Alcatel-Lucent ensures that the network will function as per the specifications and that it will meet project objectives for quality, schedule and budget. Alcatel-Lucent fully understands the complexity of integrating large complex networks. Alcatel-Lucent has the ability to efficiently design and implement the proposed broadband data solution and backhaul network in a high-quality, timely, cost-effective manner. Alcatel-Lucent will follow well-established industry practice processes and procedures for the complete design and deployment of the Public Safety Broadband Network. The steps described below are included within the process.

#### ***a. Tower Site Survey***

- If new cell sites are determined to be needed for the LTE cellular radio equipment, Alcatel-Lucent will perform site surveys at points determined to be valuable within the RF planning effort.
  - Conduct a site surveys to determine unique characteristics and conditions which will affect site design.
    - Collect, organize, and analyze all pertinent information required to prepare lease exhibit, permit/construction drawing packages.

#### ***b. RF Engineering***

- RF Planning is described in Section D.

#### ***c. Site Implementation & Outside Plant (SIOP)***

If cellular towers are determined to be needed to support Pembroke Pines' LTE network, then Alcatel-Lucent will prepare the site surveys and tower designs and perform the construction for the site and towers.

- Drawings, including construction drawings, Zoning Drawing package, Tower Foundation Designs and any forms required by the FAA
- Surveys including a limited boundary survey, Phase I Environmental Site Assessment (ESA), a Phase II assessment if required, the FCC Checklist for the National Environmental Policy Act (NEPA), additional jurisdiction-surveys (State Historical Preservation, Archeological, Architectural, Tribal Historical Preservation, Electro Magnetic Field), and a geotechnical survey.
- Construction services such as Coordinate all underground utility locating, Design and build to the local wind speed standards for the area,
- Furnish and install towers according to the designs following all local code.

#### ***d. Engineering and Installation***

- Alcatel-Lucent will install and test LTE communications equipment in Pembroke Pines' network as more specifically described in the sections below. Alcatel-

Lucent collects and assesses information about Pembroke Pines's on-site and equipment conditions to identify site requirements that may impact the overall deployment. Based upon Pembroke Pines input and applicable equipment requirements, Alcatel-Lucent will prepare detailed specifications and order the required materials to enable efficient installation upon delivery. Once the equipment and the job are engineered, Alcatel-Lucent begins the installation of the equipment, performing the assembly, cabling and wiring, and testing of the hardware components, verifying that the equipment is functioning as engineered and specified.

- Engineering provides system designs that meet Pembroke Pines specifications and requirements with technical requirements and interfaces of ALU provided outside vendor purchased items, functional system and station diagrams, a bill of materials, and integration and field test requirements.
- Equipment Site Survey to assess physical location and to determine recommended placement, layout and cabling of new equipment. .
- Staging includes all phases from the generation of the purchase order (PO) for purchase of equipment and devices, obtaining permits, licenses, and variances, if required, Providing complete and accurate configuration information prior to the start of staging, preparing a Method of Procedure (MOP) and obtain Pembroke Pines sign-off, Receiving and inventorying material at staging site, Installing, powering and loading software and configuration files into required modules into specific units, and verifying alarm settings.
- Equipment Installation of all in-scope system hardware by running and connecting and labeling equipment power and ground drops and connecting cables from installed hardware, performing basic power-up and green light testing of in-scope system equipment purchased prior to integration, and obtaining Pembroke Pines acceptance/sign-off/job completion notice at installation completion.
- Integration and Interoperability Testing (IOT) that includes testing new hardware, software or architecture changes in a live environment before they are introduced into a production network. A detailed operational and inter-working feature test design for all purchased (Alcatel-Lucent and third party) and existing equipment will be provided along with progress reports and test results will be provided to Pembroke Pines as completed.

#### **G. Operations, Administration and Maintenance (OA&M)**

Waiver Recipients should provide a brief description of their planned network operations capabilities, including systems and processes related to network management, special operations and coordination or interoperability with other networks, administration/provisioning, and maintenance. They should demonstrate performance reporting capabilities if planned. They should also address the operational aspects of security. Waiver Recipients should address operational aspects of interoperability and flag any potential issues to arise for future development of nationwide network.

Pembroke Pines will engage Alcatel-Lucent to administer, manage and maintain its Public Safety Broadband network. As a network system integrator with many carrier and enterprise Pembroke Pines that outsource their voice and data network management to Alcatel-Lucent, the company has considerable experience in managing all facets of the proposed project to ensure continuity and consistency across all resources devoted to the project and to be the single point of contact.

Alcatel-Lucent WILL support Pembroke Pines as additional operational and growth demands on the new network arise.

Alcatel-Lucent also provides, as an option, post commissioning services such as network operations services, network maintenance and network outsourcing (Build, Operate & Transfer or Build Operate & Maintain). Network operations services provide the remote, real-time performance monitoring and fault resolution of contracted network elements from the Alcatel-Lucent Global Network Operations Centers (GNOCs), the delivery of network reports, remote backups of network element configurations, network element configuration changes and network performance analysis.

#### Network Monitoring and Fault Resolution:

- Establish Data Communications Network (DCN) Connectivity to all monitored elements.
- Setup all elements for Remote Network Monitoring Service and develop Operations Readiness Testing (ORT) Plan and Joint Operations Plan (JOP) including a comprehensive series of tests to exercise the network, staff, processes, and support systems in validating Business Objectives with the plan for information exchange and interfaces.
- Provide 24x7x365 remote monitoring of all in-scope network equipment via ping monitoring and Simple Network Management Protocol (SNMP) for each object under management to determine device health, connectivity, and availability. Ping intervals will be set for the most efficient levels based on the install base and bandwidth availability. Acknowledge Alarms according to standard targets. Provide verbal and/or electronic notification to Pembroke Pines of the outage (time of outage, and scope of outage, and potential outage duration).
- Identify and acknowledge Faults by manual or auto creation of trouble tickets in the GNOC trouble ticketing system.
- Perform routine diagnostic procedures to clear troubles and retire alarms.
- Manage trouble ticket updates and case-manage problems through resolution.
- Conduct diagnostic tests to isolate communication failures.
- Isolate each incident or outage and take all necessary remote and/or field actions necessary to restore network and equipment operational functionality according agreed upon severity levels and Service Level Agreements (SLAs)

For network maintenance, Alcatel-Lucent provides an extensive field and remote maintenance portfolio servicing some of the largest telecommunications service providers in the world. Today, Alcatel-Lucent operates more than 220 service centers and supply depots within the United States. Their maintenance program can be tailored to include full turnkey support, including a spares depot, remote network monitoring, remote level 2 and 3 technical support and trained dispatch personnel located in the area with pre-positioned replacement materials to support rapid response and replacement of inoperable or damaged equipment, along with remote maintenance support for software upgrades as necessary. We utilize performance reports with sophisticated models to identify necessary preventive maintenance. Redundancy designed into the network and field infrastructure accommodates maintenance activities.

#### Technical Support:

- Alcatel-Lucent's Technical Support (TS) Service provides those operating Pembroke Pines' network remote access to Alcatel-Lucent engineers in support of product-related questions, troubleshooting assistance, diagnostic procedures, and Patch Releases and Maintenance Releases to restore and resolve network troubles for Maintained Products. For Severity Level Critical (Severity 1) and Major (Severity 2), restore Maintained Products to operational status by identifying defective hardware components or providing software and/or procedural workarounds, where feasible. If Alcatel-Lucent determines it cannot restore or resolve an issue remotely, Alcatel-Lucent will provide emergency on-site support.

#### Repair and Exchange:

- Repair & Exchange Services (RES) provide repair or exchange of defective, Pembroke Pines-owned hardware (Parts) for the in-scope network equipment. SLAs include various options for Advanced Exchange (RES-AE) and Return for Repair (RES-RFR).

Several of the key tools supplied by and utilized by Alcatel-Lucent in the management of Pembroke Pines' network are described in the next sections.

#### Element Management System:

The Alcatel-Lucent network uses the 5620 Service Aware Manager to manage most of the network elements, including the eNB, the backhaul routers and microwave equipment, the MME, the S-GW and PDN-GW, and the PCRF. This simplifies operations and minimizes integration operational expenses. 5620 SAM provides a comprehensive end-to-end management solution spanning mobile and transport network layers, and leverages knowledge of transport infrastructure to provide a correlated view of the impact of failures in transport layer on the mobile layer, as the Mobile-Transport relationship is discovered dynamically. This simplifies fault isolation - transport layer is immediately implicated / absolved in failures at the mobile layer

The 5620 SAM extends the EPC FCAPS solution to include the radio access - all under a single management system, and provides the following capabilities and benefits:

- Network Element Mediation
- Configuration Management
- Network Element Security Configuration
- Activation Management
- Call Trace Management
- Supports 4G SON Functions (ANR, Self-Configuration, PCI)
- PCMD Management
- Fault/State Management
- Performance Data Collection
- OAM Test Management
- Northbound Interface - 3GPP compliant I/F
- Wireless tool chain integration - WPS, NPO, eDat

#### Network Performance Optimization:

The Network Performance Optimizer (NPO) uses a rich combination of performance and fault management data (Per-call measurements, counters, configuration, call trace and outages) to assist in performance reporting, optimization and troubleshooting of both e-UTRAN and EPC. It computes valuable Key Performance Indicators (KPIs), provides

reports on congestion/traffic, capacity/load, mobility, quality, accessibility and retainability and allows for both reports and graphs customization.

#### Subscriber Data Management:

The Public Safety operator can leverage the same authentication and mobility mechanisms used in commercial networks to enable seamless roaming across jurisdictions, as well as within commercial networks. The Home Subscriber Server (HSS) contains user information related to service provisioning, and LTE network elements use this information to handle calls or sessions, to locate and authorize users, whether they are roaming in home networks or visiting other networks. In the Alcatel-Lucent network, the HSS also contains the Subscriber Profile Repository data associated with the PCRF. The Alcatel-Lucent HSS is based on the Alcatel-Lucent 8650 Subscriber Data Manager and leverages the same high-availability ATCA v2 platform used for the MME.

#### Device Management:

Device Management becomes more important in the LTE broadband environment than in previous generations of mobile wireless technology as the number of broadband applications increase. The devices contain very sophisticated subscription containment hardware and software to support both device programming and specialized application loading. The Motive architecture provides an integrated solution that spans not only device management per 3GPP and OMA standards but service management as well. The Motive solution includes a service management platform that supports operator interfaces, Pembroke Pines service support and self-service access to reduce operating costs. Motive includes a Mobile Device Manager to manage the provisioning of devices and supports a large variety of interfaces to Pembroke Pines relationship management (CRM) systems that map from subscription to subscriber configuration. The Motive solution includes support templates for a variety of operator programmable device configurations, device descriptions, email settings, handset programming templates to provide flexibility, and repeatable provisioning for devices and applications.