August 12, 2009

From: AD HOC Team on User Requirements
Stu Overby - Team Leader
Ahsan Baig - City of Oakland, CA
Donald Denning - City of Boston, MA
Gabe Elias - Albemarle County, VA
Al Ittner - Motorola

To: Dan Hawkins, Chair - Operations WG, NPSTC BBTF
Dave Troup, Co-Chair - Operations WG, NPSTC BBTF

cc: Dave Buchanan, Chair – NPSTC BBTF

I. PROCESS

The AD HOC team on User Requirements has developed the attached list of requirements, based on 1) a review of the 700 Broadband waiver requests submitted to the FCC; and 2) operational experience of the public safety practitioners on the AD HOC Team. The information below also includes some background and explanation of the AD HOC Team results.

The AD HOC Team relied on individual contributions to develop its work and held two conference calls, an initial one to agree on a process and action items and a subsequent call to review member contributions.

II. GENERAL RECOMMENDATIONS

During the discussion, public safety practitioners noted that the requirements will vary depending on the proximity of a public safety entity to its home jurisdiction. The most complete set of broadband requirements are needed within the home jurisdiction, i.e., within the coverage footprint of the home system, and in close proximity to the home jurisdiction for local area prevention and response. A subset of those requirements will need to be accessible while roaming to a more distant jurisdiction, including access along major highways enroute. Users traveling from one geographic area to another by vehicle may move through multiple areas. While the requirements may be different when they reach their ultimate destination, they are likely to need some type of basic access to obtain services while traveling through other networks. Roaming access while in a distant jurisdiction should include unrestricted IP routing and generic access to the internet. When traveling to a jurisdiction outside the home area for the purpose of providing mutual aid assistance related to a specific incident, the roaming user will likely need access to databases and other information routinely available to the jurisdiction where the incident is occurring. This will entail the need for more rigorous security and authentication than that needed for more casual roaming situations.

The exact subset of requirements needed for roaming could vary across jurisdictions, as the operational needs of jurisdictions vary. Accordingly, the AD HOC Team believes that NPSTC BBTF final recommendations should identify a basic set of common applications for roaming initially, and should also note that jurisdictions require the option to deploy their own additional applications beyond the basic set required for roaming, as operational needs dictate. Over time, after experience is gained across multiple jurisdictions with deployment and actual use of broadband systems as authorized through waivers and/or rule changes, the public safety community may determine through experience that additional applications should be added to the basic set initially identified for roaming. This could be done through a joint consensus of the jurisdictions with operational systems and the PSBL.

The AD HOC team also recommends that the FCC rely on the public safety community in coordination with the PSBL to identify the basic set of roaming applications, rather than defining the applications in the rules. Following such an approach places the decision where the greatest operational expertise resides and enables a faster more streamlined process for any necessary modifications as experience is gained through actual deployments and use of the 700 MHz broadband facilities.

III. SUMMARY OF PUBLIC SAFETY REQUIREMENTS AND APPLICATIONS IDENTIFIED IN 700 MHz WAIVERS

Database Access in field:

- Internet and intranet access
- Criminal databases for suspect information
- Police officer lookup of DMV records
- Mapping/GIS
- Report management system access
- Incident management databases
- Access routine criminal justice data such as photographs to identify individuals
- Telemetry/remote diagnostics
- EMS officials can access other public safety departmental pre-plan information, national databases and mapping information
- EMS officials can access patient records to retrieve patient history whenever the patient is unable to verbally communicate.

High speed file download and upload:

- Distribution of images, including mug shots and incident stills
- Battalion chief at an incident could download critical building floor plan information
- Police officer could download key investigative data

- Fire officials can access pre-planning and mapping data from a centralized server to fire vehicle to have most current information (rather than store on vehicle computers as they now do).
- EMS officials can have instantaneous bi-directional communication of patient status to hospitals and public health officials
- Dispatch can distribute images floor plans, mug shots, incident stills to responders to provide a common operating picture

Video download and upload:

- Real-time streaming video / ad hoc video casting
- Improved situational awareness using video technologies
- Battalion chief at an incident could upload video to incident command
- Incident commanders to view video on the fire ground and simultaneously feed the fire ground video back to the Fire Command Center
- Dispatch can distribute surveillance feed videos and on-scene videos to responders to provide a common operating picture

Real time asset tracking:

- Tracking of assets, firefighters and resources throughout the region
- Automatic vehicle location

IV. PUBLIC SAFETY BROADBAND APPLICATIONS IDENTIFIED BY PRACTIONERS IN THE AD HOC TEAM, BASED ON OPERATIONAL EXPERIENCE

Text/Messaging/Email

- Network should support SMS-like text messaging between subscribers
- Capabilities should be provided to public safety visitors as well as home users, between subscribers and to/from NOC/dispatch centers
- Network should support "cell broadcast" functionality with the operational capability to target all users on the network, groups of users in specific area(s) and to direct messages to just public safety subscribers, or to others using the system, or to both groups. These options should be accomplishable without overwhelming the network.
- Ability for a control point to send messages to anyone on a specific network even if they are not affiliated
- Ability to know who is on a given network, including when they arrive and when they leave
- Ability for an end user to message out to anyone on the network (Calling Channel)
- Ability for an end user to message to another end user (this calls for a nationwide ID system of some sort)

- Ability for an end user to message to a group of Ad Hoc dynamic groupings
- Ability to define dynamic "channels"
- Ability for an end user to message to home network
- Ability to message to terminals within a specific geographic area.
- Email would be available either thought native network or web access

Data

- Any NLETS/NCIC access has to go through the user's home network due to auditing requirements. This isn't a problem as long as a user's home network was accessible from the host network while roaming. Currently, a mixture of Private IP Cloud and Internet VPN access is used. However, some users are moving towards the pure Internet VPN model to simplify access and become system operator agnostic.
- Once users have IP access they should have access to all their native applications which are deployed on their platform, if their home platform is IP based.
- Ability to access standardized web services for certain functions.
- "Hotelling" architecture on an "AWAY" system would allow for the creation of secure tunnels and provide the end user terminal with access to local information (such as document repositories, pre-plan, IAPs, and other data relative to the incident. It would also allow for authentication of users responding to an incident.

Video

- Traffic cameras provide big operational bang for the buck. Need ability to see basic public traffic sites, such as TrafficLand. (MESA SoR, A.22)
- Incident video backhaul; IAN video probably local…2.4/5.8/4.9GHz
- Allow for device-created incident video back to command post if no other Incident Area Network (IAN) is available.
- Allow for IAN to send video back to EOC/ECC/NOC via 700 BB if no other JAN/EAN available (MESA SoR A.18-27)
- Operational: EOC/ECC/NOC/ICP ability to send out images, plans, videos, etc. to field users efficiently (~See MESA SoR A.30.2)

Broadcast/Multicast

- Ability for an end user to broadcast an Emergency Call
- Network should support broadcast and/or multicast (depending on scenario) of binary data, in addition to "cell broadcast" of text data
- Ability for agency-hosted application to "push" binary data from central host to multiple subscriber devices (home and visitor)

AVL/GPS/Location

- Network owners/managers need to know the location of home and visitor subscribers for operational planning, asset management, etc.
- Network should provide the home or roaming subscriber with his or her location
- Network should allow subscribers to provide their locations to the network and be able to differentiate between public safety and other categories of subscribers.
- The network should, in turn, allow programmatic access to that application by the network owners/managers
- Ability to obtain some type of location information while moving through networks. Not everyone will have GPS but knowing roughly where you are based upon the network's idea of where you are located would be useful if lost. If you know roughly where you were, you could use Mapquest or Google maps to get directions if you had network access.

Voice

- If a network provides cellular or PTT voice, the following capabilities should be considered.
- Capability for PTT audio to be centrally monitored by a dispatch center, much like the 800 MHz 8CALL90 national interoperability channel
- Default destination for emergency traffic (see MESA SoR - TS 70.001 v3.3.1 section A.17)
- Ability for visitors to hail/request help, offer assistance, or announce pre-arranged arrival and request assignment
- If traditional dial/cellular voice provided, provide a 3 digit number to the same dispatch point, without having to dial 9-1-1
- Ability to patch cellular/PTT voice audio into area LMR systems
- Basic voice interoperability for visiting public safety users

Security- Authentication and Encryption

- Encryption should be end-to-end. This might call for local IPSEC type tunnels for authorized users while roaming into an "AWAY" response area. Certain features should be available without the needs for encryption such as broadcast messages, emergency calls etc., similar to the restriction against encryption on current interoperability channels. A PKI may work well for this as long as a national PKI is architected.

Unauthenticated Devices

- The network should provide an access method for devices which cannot authenticate themselves. Example: IP radio gateways that are not PC-based—will get address on the network or sits waiting. This allows for application-specific device servers to use 700 BB IP connectivity to create voice and other interoperability networks

Voice Gateways; Satellite Gateways, etc.

- The network should include provisions for satellite gateways to enable the option for satellite backup provisions that would be helpful in the event terrestrial infrastructure becomes unavailable due to extreme natural or manmade disasters.

Network Discovery Tools.

- Regional public safety host agencies need tools to provide information on both home and roaming usage, any outages, and general operational statistics. Similar information is available on regional narrowband trunking systems and provide agencies with key tools to help ensure reliability and planning.

***