Minnesota Department of Public Safety

Public Safety Wireless Data Network Requirements Project

Needs Assessment Report

Phase 1-Task 4/Deliverable 2

Mark Navolio
Televate, LLC

May 27, 2011

7700 Leesburg Pike
Suite 270
Falls Church, VA 22043

M.: 703-639-4200
F.: 703-992-6583
www.televate.com

Table of Contents

1 ACKNOWLEDGEMENTS AND CONTRIBUTIONS

Televate would like to express our appreciation for the valuable feedback and insights provided by the survey participants. The authors have made every effort to accurately represent the collected requirements in this report.

Participants	Representing
Robert Johnson	Bureau of Criminal Apprehension
Kurt Augustin	Bureau of Criminal Apprehension
Donald Cheung	Bureau of Criminal Apprehension
Micah Myers	Central Minnesota Regional Radio Board; City of St. Cloud
Rick Wyffels	City of Alexandria, Chief of Police
Wayne Kewitsch	City of Richfield, Fire Department
Michael Risvold	City of Wayzata, Police Chief
Cari Gerlicher	Department of Corrections
Scott Corbo	Department of Corrections
Brian Askin	Department of Natural Resources
Pat Coughlin	Department of Natural Resources; Minnesota Interagency Fire Center (MIFC)
Brian Kary	Department of Transportation
Cory J Johnson	Department of Transportation
Dan Ross	Department of Transportation
Jakin Knoll	Department of Transportation
Jim Mohn	Department of Transportation
John Moreland	Department of Transportation
Mark Gieseke	Department of Transportation
Paul Weinberger	Department of Transportation
Tom Weiner	Department of Transportation
Mark Dunaski	Minnesota State Patrol

Steven Bluml	Minnesota State Patrol
Brandon Abley	Emergency Communication Networks
Ron Whitehead	Emergency Communication Networks
Robert Dahm	State Fire Marshall
Jackie Mines	Emergency Communication Networks
Troy Langlie	Grant County Sheriff's Office
Roger Laurence	Hennepin County Sheriff's Office Metropolitan Emergency Services Board
Chris Kummer	Hennepin County Emergency Medical Services
John Dooley	Minnesota Homeland Security Emergency Management
Kris Eide	Minnesota Homeland Security Emergency Management
Monte Fronk	Mille Lacs Band of Ojibwe Department Public Safety
Lou Mosely	Minnesota National Guard
Troy Tretter	Minnesota National Guard
Teri Alberico	Minnesota National Guard
Darlene Pankonie	Next Generation NG911 Advisory Committee; Washington County 911 Center
Pat Novacek	Northwest Regional Advisory Committee
Mark M. Nelson	Office of Enterprise Technology
Russ Reilly	Office of Enterprise Technology
Ullas H Kamath	Office of Enterprise Technology
Dave Wright	US Army Corps of Engineers
Joe Snyder	US National Park Service, Midwest Regional Office
Reed Anderson	US National Park Service, Midwest Regional Office

2 EXECUTIVE SUMMARY

This report is a deliverable for the State of Minnesota Public Safety Wireless Data Network Requirement Project to convey the determined public safety user needs throughout the State. The data collection tools used for this project included both face-to-face interviews and a web based survey conducted between December 2010 and January 2011. Face-to-face interviews were conducted for state agencies and selected regional and local agency stakeholders.

The views and needs of 42 survey participants and 175 web survey respondents are represented in this report. The web survey included participants from each region of Minnesota. Today, wireless data needs are being met using Wi-Fi, commercial cellular and private data systems. The majority of web survey respondents use Verizon Wireless and Sprint Nextel for commercial wireless services.

Our study finds that needs throughout the State are largely consistent. For example, law enforcement personnel in metropolitan areas and rural areas alike have need for the same applications and have interest in the same types of devices. Public safety throughout the state identified a number of scenarios in which wireless data, especially broadband wireless data, would benefit operations. Major incidents such as flooding, school shootings, tornados, pandemics, large HazMat incidents and/or fires are incidents where a substantial amount of wireless data communications is required. The Needs Assessment is segmented into six main subject areas; Operational Requirements, Coverage Requirements, Capacity Requirements, Devices, Security and Applications.

Ultimately, the core operational need among those queried is the availability of service. The two essential components of service availability are the network reliability and availability of throughput. The stakeholders are split with regards to the required network availability. Most indicated that the network needs to be highly reliable – comparable to the ARMER network[1], while others indicated that commercial cellular grade of service is acceptable[2]. Others indicated that the network must be 99.999 percent available if it is to support mission critical voice. In many cases, the network may be available (in service), but inaccessible due to congestion as users cannot acquire the needed data throughput.

The stakeholders, with one exception, identified the need to acquire priority service for public safety above the needs of the public. In addition, the stakeholders identified a need to be able to modify priorities on-the-fly depending on incident requirements (e.g., in one incident law enforcement may need priority, whereas, in another, fire may require priority). Those queried identified multiple incidents where commercial services were unavailable due to network congestion.

Wireless data coverage, or service area, is yet another aspect of service availability. Without access to the wireless data system, public safety communications is hampered. State-wide coverage was identified as a key user need. While the state's metropolitan areas enjoy high levels of wireless data services from multiple commercial carriers, rural coverage is lacking. Some agencies have resorted to equipping their employees with multiple air cards as a hedge. The stakeholders were unanimous in their

[1] We suspect that the perceived and delivered uptime is 99.999 percent, however, per OET, the designed uptime at the edge is 99.9 percent availability.

[2] Commercial cellular availability was estimated at 99.5 percent uptime.

desire for state-wide coverage; however, they varied on the extent of the coverage. Some felt that ARMER level coverage is needed (95 percent coverage on a county-by-county basis) while others felt 95 percent overall statewide coverage is sufficient. In addition, there were differences of opinion on in-building coverage. Some felt outdoor mobile (similar to ARMER) is sufficient; while others indicate in-building coverage is required. Statewide in-building coverage at 95 percent of each county was the most demanding reported benchmark. Rural users were most affected by the lack of coverage afforded by the commercial carriers in their counties. Metropolitan users were mostly concerned about the lack of priority access to wireless services.

The capacity of the network must accommodate the user needs at a major incident. A substantial amount of usage in a small area is the most challenging scenario for a wireless broadband network. During the face-to-face interviews, an active shooter scenario was explored in detail as such an incident. Televate documented throughput requirements from the incident users to the cell towers (uplink) and from the cell towers to the users at the incident scene (downlink); all calculations assumed a completely private network for public safety personnel only. Based on this incident, the resulting baseline capacity for a metropolitan area is 4298 kbps on the uplink and 7596 kbps on the downlink. The baseline capacity for a rural area is 197 kbps on the uplink and 2509 kbps on the downlink.

Many of the anticipated applications will be developed over time. For example, helmet or lapel cameras streaming video make up a substantial amount of the incident capacity, yet they are not envisioned until the applications and technology are reliable and the funding becomes available. The incident usage in the near-term based upon existing off-the-shelf capabilities is expected to be 623 kbps on the uplink and 3849 kbps on the downlink. The capacity needs of the users will then grow from these initial levels to accommodate the full-scale of applications in the longer-term. In fact, in the longer term, we would expect that other currently unforeseen applications would further drive the bandwidth required.

State public safety personnel require a diverse set of broadband devices; primarily, devices currently in use on today's commercial wireless networks. This set of devices includes smartphones, USB and PC Card modems that plug into laptop computers, embedded modems inside laptop computers (or other form factors such as tablets). Web survey respondents prefer smartphones and embedded modems for their future needs. In fact, the number of smartphones is planned to rise by 50 percent by 2015 compared to current levels.

Several new device types were identified requiring embedded modems such as ePCR (Electronic Patient Care Reporting for biometric life signs) and offender tracking bracelets. For those agencies with existing wireless services, general projections estimate a 25 percent growth in the overall number of devices. The perspective of the stakeholders was that all devices should be able to roam onto commercial devices, but not all devices would actually require roaming with a statewide network in place.

In addition, interview participants felt that direct mode communications[3] will not be required until a broadband network replaces the current Land Mobile Radio voice communication. Such a transition is not expected for ten years or more, and therefore, such a feature is not a short or medium term requirement.

[3] Communicating directly between subscriber devices without the need for infrastructure. For example, "talkaround" is an example of such a mode of communication.

The security and authentication requirements conveyed by the stakeholders include FIPS 140-2 needs for applications that leverage Federal law enforcement databases. Stakeholders use mobile VPN to accommodate the end-to-end security requirements of FIPS 140-2. Stakeholders required the wireless network to be fully secure for all applications. Each application generally has its own authentication process.

The stakeholders required the network to accommodate a multitude of applications including high resolution streaming video, telemetry, geographical information systems and geolocation of personnel and assets, and a host of other applications. These applications and the manner in which the stakeholders intend to use them ultimately drive the totality of the state's wireless data needs. The applications vary from encrypted access to records management systems (RMS) to email, from AVL-based services to streaming video from ePCR to database look-ups. Finally, video at a major incident was judged as "mission critical" by half as many web respondents when compared to AVL. This may be due to a current lack of understanding of the role it can play at an incident, however, given that 72 percent of the incident traffic is video, it does bring in to question how the network capacity should be sized for an incident.

As mentioned above, all regions have generally similar needs. Not surprisingly, the most glaring difference is the quantity of users. The web survey showed that 92 percent of the estimated devices would be needed in metropolitan areas[4]. However, the estimated growth in users for both metropolitan and rural agencies is similar. It is estimated by one rural agency that a typical rural county would require on average 24 MDT modems; twelve for law enforcement, six for EMS and six for Fire (one per department). If MDTs are required on all vehicles, this total could grow to over 50. If considering smartphones as well; the number of subscribers can easily exceed 100 on a county-wide basis. These estimates were confirmed by the web survey where the range varied from one to 230 devices for rural counties.

It is clear from the respondents and interviewees that wireless data services will play an ever important role for public safety. As such, there is a strong desire from this community for a comprehensive wireless data solution. This report provides these needs in carefully articulated detail in the hope that this solution is achievable either through negotiated or private means.

The following table summarizes the maximum and minimum requirements reported by survey respondents and interviewees:

[4] We cannot rule out biases due to an imbalance in response rates from metropolitan versus rural areas; the response rate from rural areas was 35 percent versus 65 percent from metropolitan areas. .

Criteria	Maximum Requirement	Minimum Requirement
Priority	Public safety must be able to pre-empt non-public safety data transmissions	Public safety requires priority over other users but not pre-emption.
Priority Modifications[5]	Public safety must be able to modify user priorities at (or for) an incident in real-time	No respondents stated any other requirement; however we suspect that a "timely" third party adjustment to priority would suffice for some.
Network Availability	Public safety requires 99.999% network availability	Public safety requires cellular grade reliability (99.5%) with increases over time as need arises
Coverage Area	95% coverage on a per county basis	95% coverage of the State; coverage gaps to be decided cooperatively
Coverage In-Building	In-Building portable coverage within 95% of the designated coverage area.	Outdoor or mobile[6] coverage within 95% of the designated coverage area.
Coverage Extension (e.g., COWs)	Portable and high mobile equipment for extending the radio coverage that is owned and controlled by public safety	Agreement with cellular operator to provide augmented coverage within a limited amount of time
Capacity	Sufficient throughput to accommodate a major incident in a metropolitan area and occurring after applications and devices mature	Sufficient throughput to accommodate a major incident in a present-term rural area; 197 kbps on the uplink and 2509 kbps on the downlink
Applications	Real-time streaming high resolution video from an incident scene	Automatic vehicle location
Devices	Commercial roaming capable devices to include smartphones and tablets with embedded modems	USB modems with commercial roaming capabilities
Integration	Devices leverage Wi-Fi and other networks	No alternate network integration required

Table 1: Requirements Summary

[5] The ultimate goal is for the priority of the user to be modified in "real-time", with session persistence (i.e. without interruption of services). At this time there is insufficient information from the vendor community to know whether this is possible within LTE systems. One potential alternative is for the new user priority to be in effect on the next session; thus requiring the user to end, then reinitiate the wireless session.

[6] Use within a vehicle but with an external antenna

3 INTRODUCTION

This report is a deliverable for contract #B51065 for Public Safety Wireless Data Network Requirement Project. The scope of work calls for Televate to determine the technical and operational requirements for a public safety wireless data network; the reports generated under this statement of work will determine the appropriate technical approach to public safety wireless data that addresses Minnesota's present and future public safety wireless data requirements. The initiative places a strong focus on the needs of public safety users outside the Minneapolis/St. Paul metropolitan area where commercial wireless data services may not currently be available or anticipated in the foreseeable future.

The needs collection phase of this project was split between state agency and regional/local agency needs. The contract called for face-to-face interviews for state agencies while an online survey was to collect wireless data requirements from regional and local agencies. The State of Minnesota management team and Televate both saw the benefits to adding other (i.e., non-state) potential user agencies to the face-to-face meetings. As a result, several local and Federal agencies also participated in the face-to-face meetings in addition to the state agencies.

3.1 Face-To-Face Meetings

Ten interviews were conducted during the week of January 10, 2011 as per the requirements of the contract. The interviews were organized in a way such that similar functional areas (e.g., law enforcement and corrections) were grouped together in the same interview. To ensure the greatest breadth of stakeholder participants, Televate conducted additional interviews at the State of Minnesota interoperability conference (two interviews were held at the conference) and later via a conference call on February 1, 2011.

A total of 13 interviews with 41 participants representing the following agencies were interviewed for this report:

- Bureau of Criminal Apprehension
- Central Minnesota RRB/RAC
- City of St. Cloud
- City of Alexandria
- Richfield Fire Department
- City of Wayzata
- Department of Corrections
- Department of Natural Resources
- Department of Transportation
- Emergency Communication Networks
- Grant County Sheriff's Office
- Hennepin County Sheriff's Office
- Metropolitan Emergency Services Board
- Homeland Security Emergency Management
- Mille Lacs Band of Ojibwa – Department Public Safety
- Minnesota National Guard
- Northwest Minnesota RAC
- Office of Enterprise Technology
- State Patrol

- US Army Corps of Engineers
- US National Park Service
- Washington County PSAP
- NG911 Advisory Committee

The complete list of attendees, the departments they represented and the schedule can be found in Appendix A.

3.2 Online Survey

The Web Survey provided an opportunity for local and regional public safety personnel across the state of Minnesota to convey their wireless data requirements. The web survey followed the same general outline that was discussed during the interviews with state agency stakeholders; however, more specific questions regarding quantities of users were asked on the web survey. The web survey request was sent out on January 4, 2011 and was closed on February 10, 2011. An email message requesting participation in the web survey was sent to over 407 public safety professionals throughout the state. A hyperlink to the survey was also posted on the Statewide Radio Board website. And lastly, the web address was posted during the Minnesota 2010 Public Safety Interoperable Communication Conference in St. Cloud.

Out of the 400+ potential participants, 171 individuals completed the survey. Figure 1 provides a summary makeup of the respondents by the type of entity that they represent.

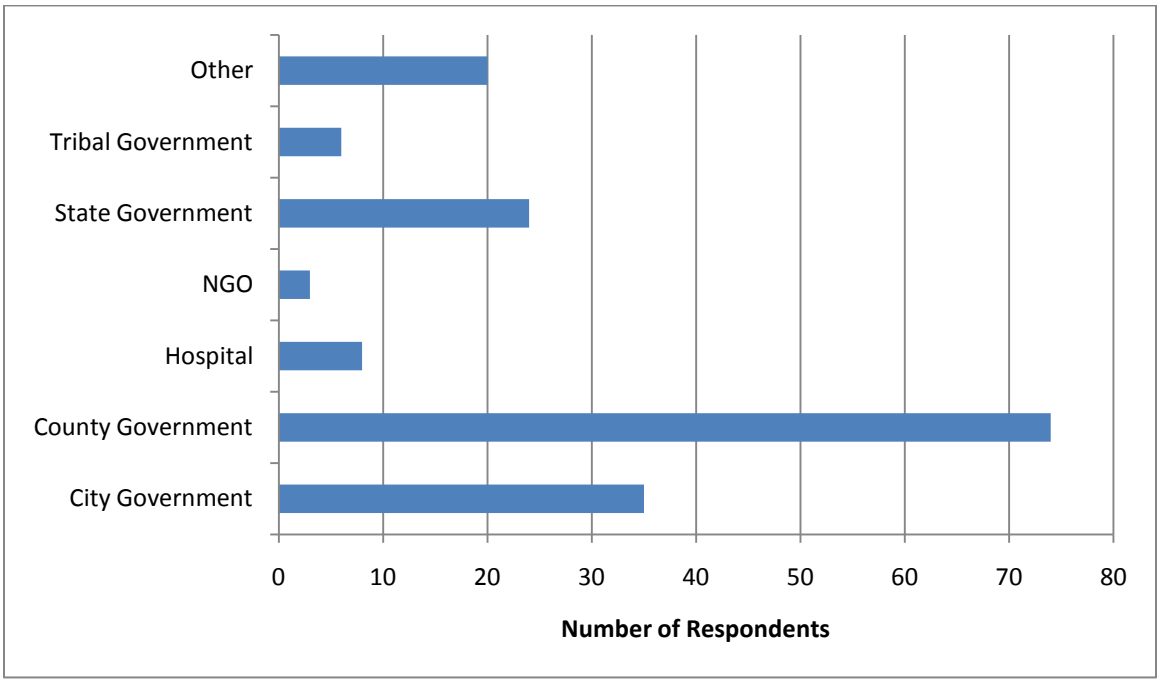


Figure 1: Online Survey Respondents by Type

Nearly two-thirds of the respondents came from County and City government – making up the majority of those participating in the survey. Other entity types included townships, joint powers organizations, Federal government, consolidated PSAP, private ambulance service, and an unorganized territory. First

responders made up the majority of respondents; 39 percent are from Law Enforcement agencies, 13 percent are from Fire departments and 16 percent are from Other Public Safety agencies such as Department of Homeland Security, Department of Corrections, PSAP, etc.

The survey also captured the type of functions the respondents represented. Figure 2 represents the results of the web survey. It is important to note that multiple responses were allowed (e.g., a communications representative might respond on behalf of the entire county government).

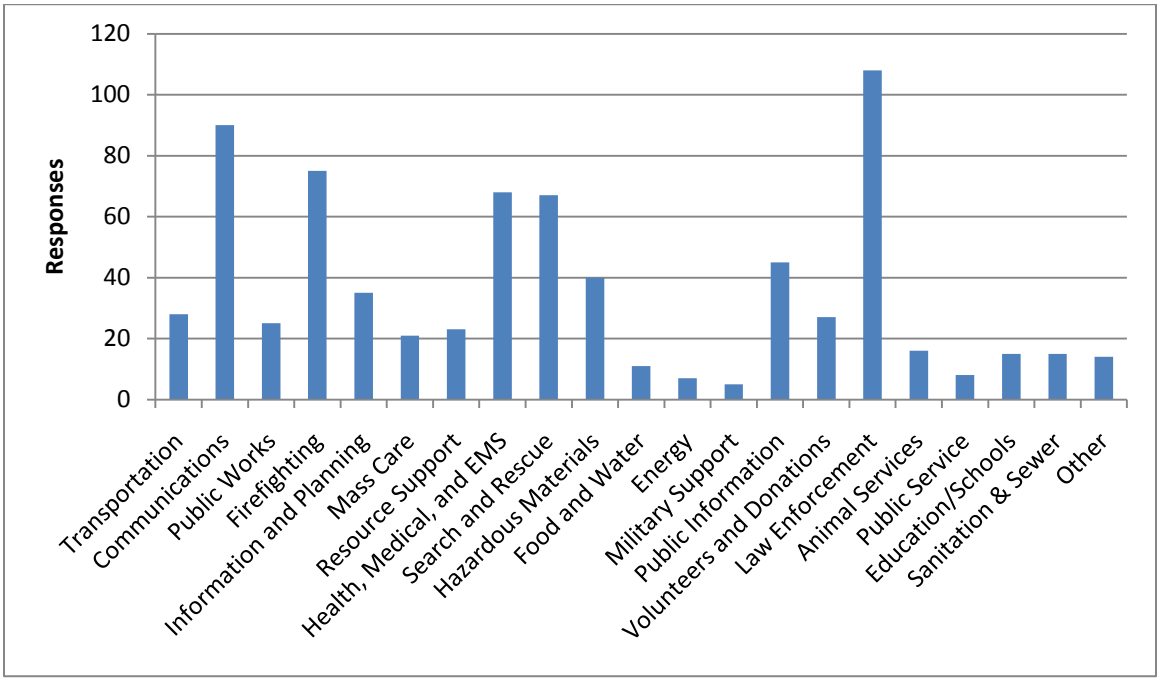


Figure 2: Functional Breakdown of Respondents

Figure 2 shows that the majority of the 171 respondents represented law enforcement interests. Other significant responses included communications, firefighting, EMS, as well as search and rescue. In the "other" category, many of the responses indicated emergency management. While the traditional "first responder" functions are the most represented, the survey did capture some response across the entire emergency support function spectrum as well as other public safety functions.

There was a concerted effort[7] to recruit respondents from outside the metropolitan areas. Invitation lists were carefully prepared to ensure geographical representation from all Minnesota counties. Respondents were also encouraged to forward the web link of the survey to other interested first responders. These efforts resulted in a response rate of 35 percent from rural areas (as designated by the US census by cross-referencing the provided zip code).

[7] Specifically, there were more than 30 invitations sent to participants from the northwest and central region.

3.3 Project Goals

The overall goal of this project is to provide Minnesota Department of Public Safety Emergency Communications Networks (ECN) with essential information required for wireless public safety mobile data planning in order to actively participate in the national wireless public safety network planning process. This project seeks to collect and document the information required to act upon present and future funding opportunities that may exist for public safety wireless data networks as a national broadband policy evolves.

The project provides ECN with an assessment of the present and future requirements for wireless public safety mobile data across the state. This assessment documents the existing local and regional needs of public safety disciplines (law enforcement, fire, emergency medical services, emergency management and public works) and estimate future requirements based upon articulated assumptions of expanded future use of wireless data to provide services to the public more efficiently and cost effectively.

The project also requires a preliminary assessment of existing commercial wireless data systems operating within the state and a determination of how well those existing services address present and future public safety wireless data needs. The project requires the development of reasonable assumptions about the potential expansion of existing commercial wireless data networks across the state and identify obstacles to commercial wireless data network expansion.

3.4 Overview

The topics covered during the interviews and online surveys covered key functional requirements that affect the levels of service and cost. The functional requirements that were reviewed are as follows:

- Network Operational Requirements
  - Service Availability
  - Service Area
  - Capacity and Throughput
- Device and Usage Requirements
- Application Requirements

Televate also asked participants “what other expectations or wireless data needs would you like this new service to address?” This question was intended to cover any other functional or operational needs that had not been otherwise addressed during the interview – perhaps offering the participants the opportunity to cover items that didn’t fit “neatly” into the prepared discussion topics.

The stakeholder interviews also included a discussion regarding the expected network capacity during a period of high demand or peak network capacity. The peak capacity is addressed in this report by assessing the aggregated wireless demand at a pre-defined incident. In any shared wireless broadband network, the capacity is limited most where the greatest demand is placed. The peak demand placed on a network defines the capacity of a system. The capacity is limited by the throughput available on each sector of a cell site.

Initially, the incident scenario discussed with interviewees was a school gym collapse. However, during subsequent law enforcement interviews, the participants indicated a limited role for law enforcement and a rather limited demand for wireless data. They suggested that a shooting incident would represent a greater load on a wireless network. Given the feedback from the stakeholders, Televate changed the focus of the analysis to the shooting incident. In order to maximize the effectiveness of the time, Televate collected high-level information on the timeline, the types of applications used, the agencies / first responders responding and the specific assets on scene that will either send or received data.

Two scenarios were then deduced; metropolitan and rural. Each scenario was further broken down to show present and future capabilities. Televate then calculated the detailed wireless data usage estimates on an application-by-application basis. The detailed findings were sent to the interviewed stakeholders for their review and validation. The suggestions and refinements were then incorporated back into the final analysis. This approach has created a more refined usage model that best represents the participants' foreseen wireless data requirements for metropolitan and rural areas.

Televate took the opportunity to collect the quantity of users per stakeholder agency to understand the makeup of the State's user community. However, this document focuses on the wireless data needs of the users, and does not endeavor to estimate the specific quantity of users or devices statewide from the various agencies as there is insufficient source data from which to extract these figures. What has been estimated is the growth rate of users and device types through a combination of stakeholder and the survey responses. This information becomes most relevant when discussing the operational and capital costs associated with different business models; the estimated quantities will be summarized when Televate reports on the implementation model. The data does provide a glimpse to those devices that are most critical to the stakeholders and survey participants.

The online/web survey consisted of 20 total questions. The survey was intended to require 20 minutes or less to complete, and therefore, was not nearly as in-depth as the face-to-face meetings. Respondents were required to answer only two of the 20 questions – those pertaining to their contact information and the type of agency they represented. Additionally, respondents were able to check multiple boxes where appropriate. As a result, the quantity of responses will not match between questions and the correlation between response quantities may not provide meaningful information. The full list of questions and their responses can be found in Appendix D.

The following sections provide the results of the interviews grouped according to functional areas of the requirements. They are segmented by the following sections:

- Network Operational Requirements
- Devices and Usage Scenarios
- Applications

4 NETWORK OPERATIONAL REQUIREMENTS

The network operational requirements encompass those items that affect the service levels of the public safety wireless data service overall. The following sections detail the network operational requirements including:

- Service Availability
- Service Area
- Capacity and Throughput

4.1 Service Availability

The service availability is a combined measurement of the end-to-end availability of the network and the service availability; the wireless coverage area or service area. Ultimately, public safety personnel must be able to communicate where needed and when needed. This section highlights the user feedback regarding the required availability of the wireless data service. It is divided between the area to be serviced, and the reliability of the area serviced. In other words, what areas need wireless data service, and, when such service is established, at what reliability shall the network continue to provide service in that area.

4.1.1 Network Availability

The network availability is a measurement of the percentage of time the network is capable of providing service. The availability measurement is a measurement of the network's reliability; however, it incorporates all planned outages as well. The network reliability refers to the extent to which the network operates in the manner in which it is intended; if the network suffers from an event that prohibits normal operations, then the measured reliability of the network is reduced. This is an important distinction, as it incorporates the end-to-end reliability and all network devices in between.

In terms of a future statewide wireless service, there are three factors that need consideration:

- Network outages due to unplanned events
- Network outages due to planned events, i.e. maintenance
- Massive network congestion that reduces the quality of service available to public safety personnel

4.1.1.1 Unplanned Outages

An unplanned outage refers to an event on the network that prohibits its operation. Events can vary from network equipment failures to a loss of power at the site. The experience of the stakeholders regarding the commercial service reliability has been generally positive. Respondents indicated that most commercial networks have been highly available (outside stated congestion and coverage issues discussed below). One stakeholder did relay a particular problem they had experience with Sprint. According to the stakeholder, after a "network change" their VPN software was unable to connect

through to their agency's network. The carrier was not able to resolve the problem and the agency was eventually forced to switch cellular carriers.

The end-to-end availability calculations were not provided for the ARMER network; however, OET did relay the reliability of the backhaul that is used to interconnect the ARMER sites. The central fiber core had been built to a reliability rating of "four-nines[8]" (99.99 percent) or better. The outer spurs, or connections to the towers, were built to "three-nines[9]" (99.9 percent) or better. It was the experience of all the stakeholders surveyed that the ARMER network exceeds its design level for reliability; no complaints (except for a single web respondent) were voiced and only positive feedback was given.

As a point of reference, prior experience with commercial cellular operators has indicated that commercial networks are generally built to a reliability rating of 99.5 percent[10] or better. The figure was later confirmed during separate meetings with AT&T and Verizon Wireless who stated that the 99.5 percent availability was a good approximation.

Most stakeholders indicated that the network should be highly reliable and comparable with the ARMER network. The implication of these stakeholders is that ARMER availability is higher than commercial services. However, some indicated that the reliability of the commercial cellular networks is sufficient for the near-term; specifically this was the feedback from State Patrol and Hennepin County who indicated that their procedures and processes do not rely upon the availability of wireless data.

However, all stakeholders, both those surveyed and the web respondents indicated that they would expect the reliability to increase over time as wireless data applications become more integrated into daily procedures and as more mission critical applications are rolled out. A key milestone would be the integration of mission critical voice whereupon the reliability would be expected to rise to five-nines or 99.999 percent or 5.3 minutes or less outage time per year.

4.1.1.2 Planned Outages

It is normal for all networks to schedule planned outages for regular maintenance and software updates. Planned outages need to be well coordinated between the network operator and the end users. Network maintenance that occurs during peak public safety activity is problematic. For example, a major system upgrade that takes a network off-the-air for several hours during peak public safety activity may severely hamper public safety operations.

In this regard, the experience of public safety personnel has been generally positive with the existing wireless carriers. The notifications provided by the commercial operators have been timely and accurate; usually providing two weeks advance notice. The agencies also have the ability to negotiate the maintenance window if necessary. The participants indicated this is an important ongoing need especially as wireless data becomes more critical to public safety operations.

[8] Reliability rating of 4-9s equates to a cumulative 52.56 minutes of outage time per year of operation.

[9] Reliability rating of 3-9s equates to a cumulative 525.6 minutes of outage time per year of operation.

[10] Reliability rating of 99.5% equates to a cumulative 43.8 hours of outage time per year of operation.

4.1.1.3 Network Congestion

Network congestion has proven to be an impediment for access to the commercial networks during large events in the metropolitan areas. Several events were proffered that describe a saturated commercial network. A primary example was the 35W bridge collapse. During the event, the infrastructure of the commercial cellular operators was fully operational. However, the networks were unavailable to nearly all public agencies because of the high demand that was placed on the systems. The commercial operators had no facility or agreements in place that would have prioritized the wireless data services to public safety personnel. So in effect, the public safety agencies had experienced an "outage of service". Several participants noted that the media would show up at an incident and further exacerbate the congestion problems of the commercial service.

In summary, it is the general perspective of the state agency stakeholders that public safety requires priority service (priority over the general public and the media), especially in the populated areas, to ensure that emergency personnel have access to information as needed over commercial networks. As commercial data use continues to grow, this issue is likely to become particularly acute[11].

4.1.2 Priority Services

All agencies surveyed expressed an interest in prioritized services and the ability to assign or change assigned priorities "on the fly." Law Enforcement expressed a strong desire for prioritized services to manage resources. Law Enforcement would like the facility to prioritize their users over non-emergency communications. To a lesser degree, State Patrol had mentioned that their officers do not rely on wireless data services for mission critical tasks; hence, prioritized services are not an obligation from their perspective. A summary of desired prioritized services is as follows:

- Top priority must be given to mission critical services during an incident.
- The ability to prioritize on a user basis over non-responders should be a requirement for all future wireless services.
- The ability of the Incident Commander to change, on a real-time basis, the priority of users and services is desired.
- The ability to prioritize certain applications or "bearer services" over another; e.g. secure RMS data over non-emergency communications services. The ability to prioritize applications is expected to be most useful during a multi-agency incident where the demand for wireless data is the greatest.

4.2 Service Area

The extent of the wireless data coverage boundary is quite important to all state and local agencies. It is the primary critique of the commercial cellular operators. Surveyed participants and web respondents, especially those working in more rural areas, indicated that coverage, or the lack of coverage, is the

[11] For example, AT&T projects 8 to 10 times data growth over the next five years (see March 21, 2011 AT&T report regarding proposed T-Mobile acquisition).

most problematic issue with commercial wireless data services. When asked about the carriers' coverage maps, most participants indicated that the coverage maps often portrayed the coverage holes, but are overly optimistic and depict coverage on maps where it is not always available. The general perception is that the maps depicted outdoor coverage, but not indoor coverage. In summary, the extent of cellular coverage has not kept pace with the improvements in commercial offerings (i.e. data-only contracts, device types and capabilities).

The general experience of the stakeholders has been that from one third to one half of the state of Minnesota lacks sufficient 3G wireless data service or coverage. The coverage afforded by the various wireless operators is inconsistent whereas each operator has regional strengths and failings. Several agencies reported that they are obliged to carry multiple wireless modems when they travel across the state as no one carrier provides the best service everywhere.

Local environs significantly affect the radio propagation of the wireless signal. From a radio propagation perspective, a single radio transmission tower can "cover" a much greater area if it is required to serve outdoor or in-vehicle devices, but not in-building users. The survey participants indicated that nearly all existing data applications are vehicle-based. The participants indicated that the level of coverage required for in-vehicle service should be used as a baseline for designated coverage areas statewide.

However, many agencies did indicate a strong desire to rollout future applications on tablet PCs for use within buildings. The surveyed participants and web respondents identified statewide coverage as a key objective for any future system. Specifically they indicated that in-vehicle coverage should be the minimum design requirement for a statewide wireless data solution. However, they varied on the extent of coverage.

Some agencies indicated that the new service must meet the ARMER requirements, where others indicated that 95 percent coverage on a statewide basis would be suitable as long as the direct input of local first responders was used to develop the coverage objective maps. The coverage of the ARMER system (the state's Land Mobile Radio voice network) is 95 percent on a county-by-county basis. More specifically, the design target of 95 percent per county is for mobile, in vehicle, usage in the rural areas and urban areas[12].

Some agencies noted that specific areas could reasonably be excluded from coverage. For example, wireless data coverage in forests is very problematic as they are environmentally sensitive areas with little infrastructure available for radio sites. Coverage on lakes and in heavily forested areas is not deemed a priority at this time. As an example, the Superior National Forest is noted as an area where State and local public safety agencies have little responsibility, and therefore, the agencies suggested that it is not practical to cover the entire forest to the same extent as a rural or metropolitan area. They proposed that it would be more cost-effective to place a priority on the vehicle trails and not ubiquitous coverage. For off-trail areas, a specialized solution could be developed for those rare occurrences when communications is needed.

The following list summarized issues surrounding some of the coverage problems and suggestions for additional coverage:

[12] LMR handheld radios have a transmit power 12 times greater than LTE user equipment, and LMR mobiles have an output power several times greater than LMR handhelds. The limitation of the LTE handset power versus LMR is the main reason LTE requires more sites to cover the same area.

- Department of Transportation would like coverage in the river valleys; Red River, Minnesota, Crow in central Minnesota and Eastern river valleys.
- Department of Corrections would like to deploy GPS tracking offender bracelets; however, the general inconsistency of wireless coverage outside of the metropolitan areas had held back its deployment.
- Several agencies noted that all state buildings should have ubiquitous in-building coverage.
- Wayzata mentioned a pending ordinance to require P25 ARMER coverage in-buildings, and envision this coverage requirement be extended to a statewide service at some point. A high priority is given to school buildings.
- Several agencies noted that handheld coverage should be the baseline.
- Fire inspectors would like to maximize in-building coverage; they generally experience insufficient coverage from all major carriers.
- Roseau County and Department of Natural Resources suggests that higher powered mobile units should be investigated especially for rural areas, to increase coverage.
- As the new statewide wireless data service would be used in tandem with ARMER, it must match its coverage at a minimum.

The following figure provides the web survey statics regarding required coverage levels:

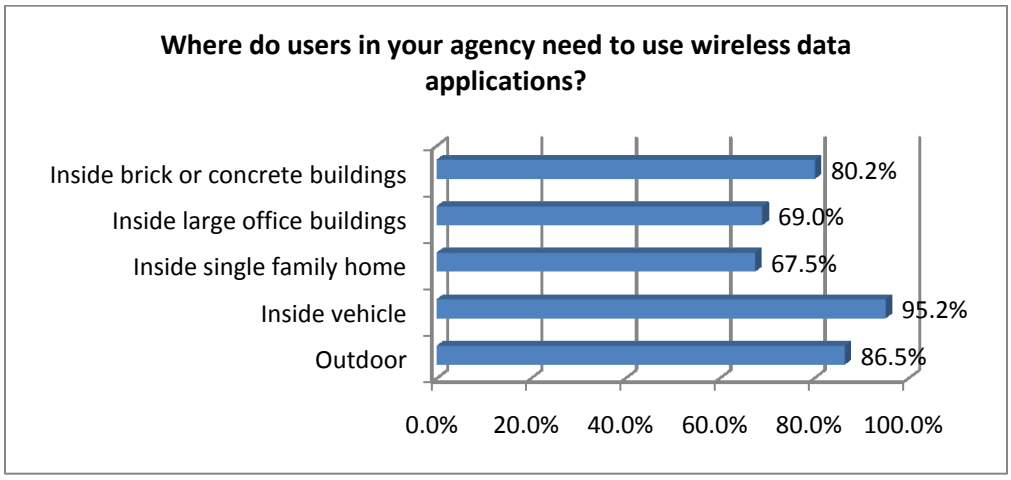


Figure 3: Locations of Wireless Data Usage

Users were able to check multiple boxes in the survey, and therefore, the cumulative total adds to more than 100 percent. The results show that greatest need is for in-vehicle coverage. More than 80 percent of respondents needed some level of in-building coverage, and more than two-thirds further specified

the in-building requirement to include large office buildings. Roughly two-thirds also required coverage in residential buildings. The web survey results show that the coverage requirement among state users is not unanimous.

In addition, the web survey yielded the following additional results regarding coverage:

- 15 percent of respondents experience little to no coverage problems
- 85 percent of respondents did experience coverage problems varying from minor coverage holes to large sections of their jurisdictions uncovered

In general, survey participants and web respondents from the metropolitan areas had placed a greater emphasis on in-building coverage as a design objective, whereas rural area stakeholders preferred to have ubiquitous mobile coverage serve as the priority.

Emergency or supplemental coverage expansion requires a physical deployment of equipment to provide service where it is lacking or to improve data throughput where it is minimal. These needs are generally met by the deployment of a "Cell-on-Wheels" (COW), Cell-on-Light-Truck (CoLT) or equivalent. The commercial wireless providers have regularly provided portable Cell-on-Wheels during major emergencies when requested. The time it takes for the equipment to arrive, from initial request to fully operational deployment, has varied from three to 24 hours depending on the location of the incident. Although the goodwill is there and the equipment is within the state of Minnesota, oftentimes, the arrival of the Cell-on-Wheels arrives too late to be of any use to public safety agencies.

Those surveyed also recognized that it is unlikely that the coverage levels of any network would be sufficiently comprehensive. Therefore, a more quickly deployable supplemental coverage solution is a high priority for the state agencies. This is especially true for emergency events in metropolitan areas where frequent network saturation blocks public safety's access to wireless broadband services. Several agencies suggest a relay or repeater to be installed on public safety command vehicles to provide commanders the ability to extend coverage in areas that do not have coverage.

4.3 Capacity and Throughput Requirements

As discussed in the introduction, the network must accommodate the user needs at a major incident. Most incidents occur within a relatively small geographical area thus creating a dense concentration of data usage usually contained within the coverage area of a single sector of a site. If the demand for data is greater than the capacity of the sector, then, the quality of service will decrease. It is for this reason the incident demand serves as one of the baseline requirements for the system.

Expected traffic density is a critical component to network capacity sizing and quality of service. A rural sector can serve anywhere from 60 to 150 square miles of service area; whereas a sector covering a metropolitan area for in-building coverage can be as small as 0.3 square miles. In day-to-day scenarios, public safety usage will be spread among many sectors – perhaps upwards of 1,500 sectors serving the entire state.

However, the usage pattern can change dramatically in the case of a major incident where the wireless demand can be within a small, localized area. In this case, the wireless services may only be served by a single sector; however, a larger incident may be served by two (2) or more sectors. Therefore, a

detailed understanding of both the required incident throughput as well as the density of the incident will provide a full scenario from which the network can be designed.

The incident was defined in cooperation with the survey participants. Televate collected the specific wireless data needs on an application-by-application basis during the interviews and then augmented the data flow characteristics into a developed model. The model considers what each user is sending and/or receiving and then aggregates the "traffic" together to determine the net uplink (data transfer from wireless device to the cell site) and net downlink (data transfer from cell site to wireless device) throughput required to accommodate the incident.

The incident models separate traffic between the direction of the traffic flow as well as the location of the end user. Two traffic flow directions are included: downlink and uplink. Downlink data is data sent from the wireless base station tower down to the end user's devices. Uplink data is path of data sent up from the end user's device back to the base station tower. The scenario assumes that the incident is taking advantage of downlink multicast video, a key LTE feature. This means that if five users are viewing the same video stream, the network would need to broadcast only one stream to the five users instead of five individual streams.

The usage is broken into four (4) separate locations. The scenario details the wireless data requirements for all agencies operating in those locations. The strike team (SWAT) is assumed to operate within the building at the incident. The incident command/unified command is located away and out of line-of-sight from the building outside the inner perimeter at the closest safe distance to the incident. The staging area is outside the inner perimeter and on the edge of the outer perimeter where space will allow the assembly of all responders to the incident. The outer perimeter estimate is the least concentrated group of users. The data usage for this group is spread out across each of the road-blocks surrounding the incident.

The web survey asked for two responses regarding a major incident:

- Describe your wireless data needs at a major multi-agency incident. This could be either a past incident or possible future event.
- How many personnel and vehicles would respond?

The web survey incidents included flooding and other natural disasters, major business fires, school shootings, HAZMAT spills, and others. The response size ranged from a few to 1,000 personnel and up to 140 vehicles. The median response size of those who responded to the question was 50 personnel and 23 vehicles. The average response was 80 personnel and 30 vehicles. These responses provide some perspective to the incident used for capacity analysis.

The incident for which the capacity analysis was conducted is an active shooter / hostage scenario at a large high school and involving casualties. The scenario includes more than 100 public safety responders representing SWAT, Law Enforcement (for perimeter security), EMS, Fire, and Incident Command / Unified Command. Given the web survey responses, these quantities fall in line with the estimated size of a "major multi-agency incident." Some incidents, such as flooding and wildfires[13], are far larger;

[13] The response regarding the wildfire required 1,000 responders and the flooding response required 250 responders.

however, because these types of incidents generally cover larger geographical areas, their demands are spread over many more sectors, and their traffic density is lower. The active shooter / hostage scenario represented an incident response comparable to the larger, but concentrated, incidents from the web survey.

The incident ramps up fully within 60 minutes and lasts 240 minutes. The incident accommodates the use of real-time streaming video, telemetry, biometrics, pre-plans, and other applications. Appendix B provides a detailed description of the incident as well as a comprehensive list of the applications needed for the incident.

Three capacity related scenarios have been considered in this report and are discussed in the following sections:

- Present Metropolitan: Applications that are deployed today and with an incident response that is indicative of a metropolitan area in Minnesota (i.e., a higher quantity of responders compared to a rural area).
- Future Metropolitan: Applications (use scenarios) that are anticipated in the future with a metropolitan area level of response.
- Present Rural: A scenario in which the response size is based on a rural area and with presently utilized applications.

The throughput requirements for the scenarios are conveyed in kilobits per second (kbps). The tables depict two separate throughput levels, peak and average. The peak levels are those that would occur if all intermittent uses of the network occurred at the same time. The average usage scenario assumes that the usage is spread out over a period of time, and therefore, do not occur at the same time. All of the cases assume a jurisdictional area network (JAN) model without an incident area network (IAN). In other words, traffic that will remain at the incident (e.g., a video stream from a strike team (SWAT) to the unified command) must be transmitted twice. Specifically, the traffic is transmitted once from the user to a base station, and another time from the base station to the recipient of the traffic.

4.3.1 Present Metropolitan

Assuming a wireless data network available in the near-term, the incident data requirements are based on those applications that are currently deployed. Applications that are designated as “future” are omitted. The resulting wireless data requirements are as follows:

Present Scenario	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
Strike Team Subtotal:	0 kbps	0 kbps	0 kbps	0 kbps
Unified Command Subtotal:	904 kbps	6849 kbps	241 kbps	3381 kbps
Staging Area Subtotal:	220 kbps	308 kbps	124 kbps	212 kbps
Perimeter Subtotal:	257 kbps	256 kbps	257 kbps	256 kbps
INCIDENT TOTALS:	**1382 kbps**	**7414 kbps**	**623 kbps**	**3849 kbps**

Table 2: Throughput Requirements for Metropolitan Areas - Present Scenario

As the table shows, the bulk of the data flows in the downlink (from the core network out to the users at the incident scene) for the initial case. The results show that the incident throughput needs far exceed the speeds established by the Broadband Technology Opportunities Program (BTOP) for broadband. Specifically, the rates are 768 kbps downlink and 256 kbps uplink. However, the BTOP levels reflect the rates available to individual users. This cumulative view then reflects roughly 2.4 times the throughput on the uplink and 5.1 times the downlink requirement when compared to BTOP rates. Importantly, the FCC recently proposed standardization around these BTOP rates, and therefore, these throughput levels may become the requirement for the State of Minnesota.

4.3.2 Future Metropolitan

The incident incorporates several applications that have not yet been widely utilized by public safety personnel. The applications have been designated as “Future Public Safety Data Services”. The “future” applications are based upon standard off-the-shelf technologies that are in common practice or use throughout industry but, for a number of reasons, are not currently in widespread use in public safety. In most cases, these applications have been tailored for public safely. A key obstacle to their greater deployment has been the unavailability and the cost of wireless data services. The additional “future” applications are as follows:

1. Helmet/Lapel cameras upload of video from Strike Team (SWAT) to Unified Command
2. Tactical Telemetry (geo-positioning) upload from Strike Team to central data server
3. Biometrics (vital sign monitoring)
4. Deployable Fixed Wireless Situation Awareness Cameras for perimeter
5. Throw Phone with voice communications discrete video for communications between assailant & negotiator
6. Audio/Video Conferencing between Unified Command & EOC
7. Video from NG911 services
8. Video from the EMS Unit to the Trauma Care Physician

The resulting wireless data requirements for a future metropolitan scenario are totaled in the following table:

Future Scenario	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
Strike Team Subtotal:	2856 kbps	492 kbps	2667 kbps	303 kbps
Unified Command Subtotal:	1106 kbps	10009 kbps	427 kbps	6524 kbps
Staging Area Subtotal:	1044 kbps	609 kbps	947 kbps	513 kbps
Perimeter Subtotal:	257 kbps	256 kbps	257 kbps	256 kbps
INCIDENT TOTALS:	**5263 kbps**	**11366 kbps**	**4298 kbps**	**7596 kbps**

Table 3: Throughput Requirements for Metropolitan Areas - Future Scenario

The table shows roughly double the average downlink throughput and a seven fold increase in uplink throughput compared to the present case. Much of that increase stems from an increase in uplink video traffic that is transmitted to incident command and other locations on the downlink. These rates are roughly 17 and 10 times the BTOP rates on the uplink and downlink respectively.

4.3.3 Present Rural

In metropolitan areas, the response to the incident can grow to be quite large as both the risk to mass causalities and the number of first responders within short driving distance is great. In rural areas the population density is smaller, and therefore, the rural response often will be limited to the reduced quantity of responders who could render aid in a timely manner. In this scenario the personnel responsible for the incident command/unified command will assume the tactical role (strike team) as soon as the situation permits it. The perimeter is limited to two (2) units. The reduced number of responders will restrict the wireless data usage in rural areas in like fashion.

The Rural Scenario is based feedback received from stakeholders from more remote regions. The list is comprised of the same applications that make up the Present Scenario above. The only difference between the Rural Scenario below and the Present Scenario above is the number of responders at the incident. The following table depicts the throughput requirements for the present case in a rural area:

Rural Scenario	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
Strike Team Subtotal:	0 kbps	0 kbps	0 kbps	0 kbps
Unified Command Subtotal:	280 kbps	5019 kbps	132 kbps	2445 kbps
Staging Area Subtotal:	0 kbps	0 kbps	0 kbps	0 kbps
Perimeter Subtotal:	64 kbps	64 kbps	64 kbps	64 kbps
INCIDENT TOTALS:	**344 kbps**	**5083 kbps**	**197 kbps**	**2509 kbps**

Table 4: Throughput Requirements for Rural Areas - Present Scenario

The table shows that the reduction in personnel results in a substantial decrease in the amount of throughput needed to accommodate the demand. The throughput requirements on the uplink are less than those of the BTOP rates, but the downlink demand represents 3.3 times the BTOP rates.

5 DEVICES AND USAGE SCENARIOS

Public Safety Personnel and their supporting agencies require a diverse set of wireless data devices. At a minimum, these agencies require devices similar to those offered by commercial cellular operators. The devices include:

- Embedded modems inside Tablets and Personal Computers (not generally user removable)
- USB, PCMCIA, or PC Express wireless modems attached to laptop (user removable modems)
- Smartphones with integrated voice and data,
- Vehicular Modems or Mobile Routers that provide wide-area connections for vehicles and may include Local Area Network support (via Wi-Fi)

The following figure provides the makeup of current devices from the web survey.

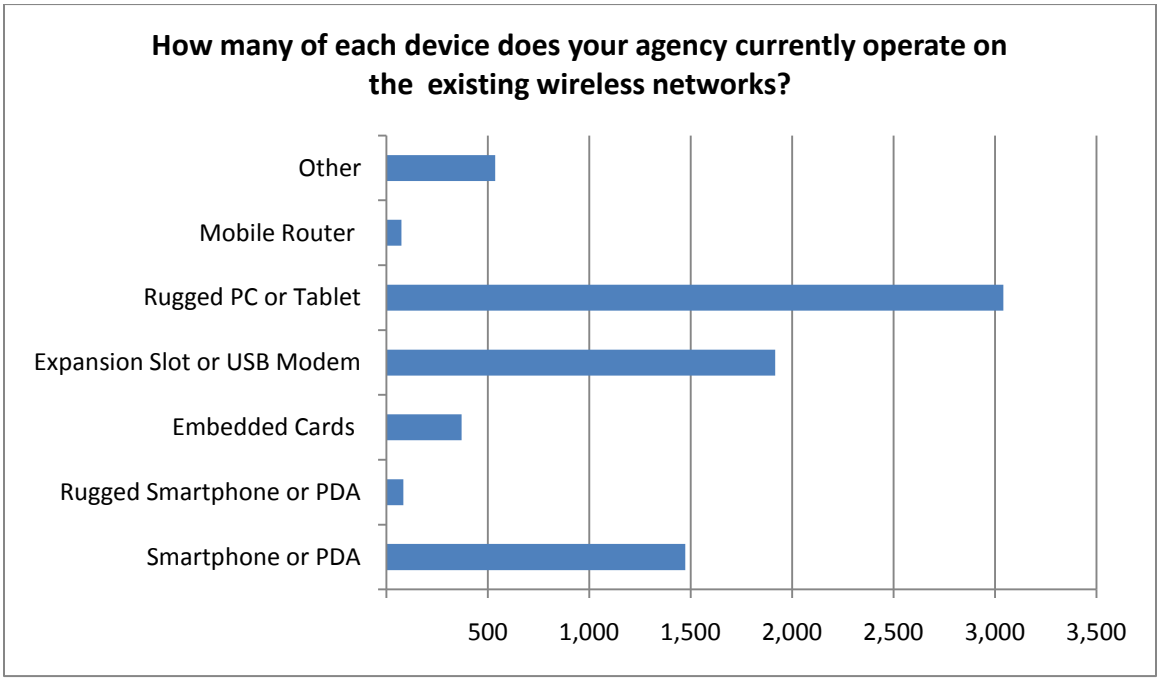


Figure 4: Percentage of Devices in Current Use

The survey results show that the rugged PC or tablet makes up the greatest number of devices. Those devices can be connected using embedded cards, mobile routers, external slots, or other means. The predominate modem mode seems to be the expansion slot or USB modem. Some agencies reported that while it is beneficial to have modems that are embedded in the tablet or laptop, they prefer field replaceable modems (e.g., USB modems) because of the rapidly evolving wireless data market. On the other hand, the agencies prefer a more robust/rugged solution. The USB modem is identified as problematic by some agencies because it protrudes from the computer and is prone to mechanical

failure. Smartphone use is also substantial with nearly 1,500 among those who responded to the survey.

5.1 Future Usage Scenarios

The Chief of Police for the City of Alexandria made a general observation that future wireless data devices will become smaller, the applications available to public safety will multiply, the cost of wireless service will reduce (in real terms) and the need for greater efficiency will increase. Hence, it is safe to assume that public safety personnel and their supporting agencies intend to use more hand-portable devices and that these devices will be more ubiquitous to public safety's daily mission critical activities. The basis of this assumption has been confirmed by several agencies who firmly stated their intention to rollout more hand-portable devices as funding comes available.

The number of usage scenarios will expand greatly in the future beyond the present day. Specifically, law enforcement agencies expressed the intent to use hand-portable tablet computers for criminal reports processing. Some law enforcement agencies are planning for future rollouts of other applications to include biometric readers, such as finger print readers. It is inevitable that in-building coverage will be a future necessity as more hand portable devices are rolled out to public safety agencies. A list of the devices that were mentioned by the survey participants and the web respondents is as follows:

Device Type	Description
Tablet computers	Handheld access to central records management databases; generally excludes a keyboard and includes a touch screen interface with otherwise similar functionality as existing laptops. Can use embedded or external modem.
Laptop/Notebook Computers	A personal computer with a large display and keyboard. Can use an embedded or external modem.
Mobile Routers	Modem with multiple ports allowing aggregated wireless connectivity. Can include several wide area modems that are embedded or external to the device.
Smartphone / PDA	Handheld device for standard cellular-like services; email, voice, GIS services, etc. generally including an embedded modem
Biometric Readers	Fingerprint readers for criminal apprehension; these devices could have wide area modems or local area modems via a connection to other wireless device
Biometric Monitors (ePCR)	Monitoring of vital signs for first responders and patients (ePCR - Electronic Patient Care Reporting); the devices could have wide area modems or local are modems connected to other devices
Wireless Cameras	Tactical or situational awareness video; portable camera, helmet or lapel camera with integrated wireless modem or equivalent connectivity to the wide area network

Device Type	Description
Offender Bracelets	Offender tracking device with integrated wide-area wireless modem.

Table 5: Device Descriptions

The common thread between each of these devices is their portability. The handheld devices will generally require higher receive level signal strength than devices with external antennas due to poorer performing antennas and other environmental losses. This requirement for higher signal strengths will have a direct impact on the design criteria or service level agreement for the new wireless services. Figure 5 indicates the anticipated future makeup of devices from the web survey:

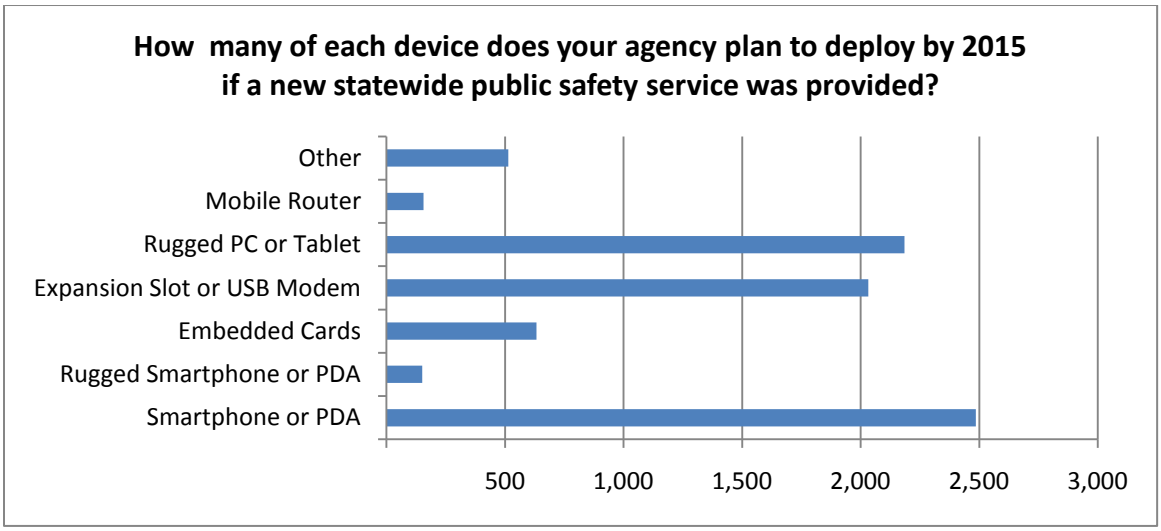


Figure 5: Planned Devices by 2015

When compared to the current use scenario, this future use shows a dramatic increase in smartphones or PDAs and a slight decline in the number of rugged PCs or tablets. This suggests a potential shift from a PC based environment to a smaller form factor handheld device. The data portrays more than a 66 percent increase in anticipated number of smartphones from today to 2015 despite fewer responses from respondents[14]. Importantly, the results also show that non-rugged smartphones/PDAs will remain the prevalent handheld platform with more than 10 times the adoption of the rugged versions.

The results also underscore the expected portability of devices in the future. The mobile router, attaching the user to the vehicle, represents one-tenth of the quantity of users of that of mobile PC based solutions or smartphones. A total of 156 mobile router devices are reported in the survey compared to 2,032 expansion slot or USB modems.

[14] A total of 95 individuals responded to the current device makeup question while only 83 responded to the future device question.

5.2 Direct Mode Communications

Direct Mode communication is a peer-to-peer communications method that does not use the wireless infrastructure. Similar to "talk-around" communications for Land Mobile Radio voice systems, direct mode for data would enable communication between two devices without "cell sites." It is generally used in areas where the connection to public safety radio communications network is unavailable due to lack of signal or a network failure. Direct mode communications was a topic that was reserved for the face-to-face interviews due to the difficulties in capturing feedback in a web survey.

The agencies surveyed did not possess peer-to-peer software applications that would be required for direct mode communications. In other words, even if devices could share data packets directly with one another, the devices generally lack the applications to make such a capability useful. The Department of Public Safety ECN summarized the need for direct-mode as being a necessity "only if a broadband data network becomes the only network." In other words, such a capability is required to share voice communications only if a Land Mobile Network is no longer in service. Importantly, there is no expressed requirement for direct mode communications for other applications. Therefore, the future requirement is for direct mode voice communications.

5.3 Roaming

Roaming is the act of operating on another (foreign) network. Usage on other public safety systems (e.g., a state network in North Dakota) is expected to be a mandatory FCC requirement to achieve nationwide interoperability. Additionally, it is likely that public safety agencies would not charge for usage on each other's systems. Therefore, Televate's roaming focus was on roaming out of state to a commercial carrier (i.e., before other public safety systems exist). This type of roaming affects both the operational cost and the device requirements. Commercial carriers will charge for any usage on their networks and the devices must be able to access the commercial carrier frequencies and technology (e.g., CDMA versus GSM).

In terms of the potential number of users, the requirement for roaming by the Minnesota stakeholders is extensive. Most agencies would like all of their devices to have the option of roaming. However the utilization of roaming is expected to remain quite small with only a small fraction of users. Some border counties and towns have mutual aid agreements and intertwined public safety operations that extend across the state lines; however, the number of users in these areas is relatively minimal in comparison with the state-wide number of potential subscribers. The two exceptions would be the Fargo-Morehead and Grand Forks metropolitan areas. In those cases, the expected "out-of-state" roaming could be substantial.

The requirement for roaming across the international border with Canada is limited. However, it is likely that Canadian public safety agencies would seek an agreement to roam onto the Minnesota network as the trans-Canada rail line extends into United States territory through Lake of the Woods County. This rail line is the main East-West freight route through Canada and carries a variety of potentially toxic materials. Likewise, the communities from Warroad to Roosevelt to Baudette have in place mutual aid agreements between themselves and Canadian officials. Therefore, incoming roaming will be critical to public safety operations in those areas.

6 WIRELESS APPLICATIONS

The following section covers both existing and future applications that are envisioned for use by participants.

6.1 Video

As we will see in the incident analysis, video presents the most demanding data application being used. Video applications can be broken down into distinct purpose-driven categories:

- Situational Awareness and Live Monitoring**:** Situational awareness video is deployed to gain an on-site viewpoint of the scene in question. It comes in many guises ranging from fixed video to mobile video sources. The most common configurations are as follows:
  - Dashboard or vehicle mounted cameras and with on-board storage (DVR) of the video data and real-time video streaming capabilities to other public safety personnel
  - Fixed building cameras (agreements permitting)
  - Fixed traffic cameras and other third party sources
- Tactical Video: Tactical video sources are those generated at the scene of the incident either by stationary or mobile elements.
  - Lapel or helmet cameras; remote users access the data directly from the device
  - Stationary tactical cameras that are deployed for a specific short-term purpose (e.g., at an incident)
  - Mobile robotic devices with camera or pole mounted cameras used in search and rescue
- Analytical Video: Analytical video begins streaming to a predefined IP destination once prompted by a predefined trigger.
  - License Plate Recognition (LPR) generally performed using on-vehicle cameras with video analysis at the vehicle. It includes bi-directional metadata transfers between the storage device and the central management server. It may also include video transmission upon a triggered event.
  - Physical Security and Motion Detection that will stream video upon a pre-defined trigger
- Forensic Video: Evidentiary video provided to law enforcement. Forensic analysis is not time critical, and therefore, it does not need to be streamed in real-time. The data may be retrieved via a wireless network or it may be transmitted for centralized storage.

Many of these video applications can impact both the uplink and downlink capacity of the network depending on how the video is used. For example, the dashboard video may be streamed to both a dispatch center on the fixed network and to a law enforcement supervisor out in the field. The latter

case would require the video to be streamed uplink to a base station and streamed again from a base station to the supervisor. The former case would require only the uplink video case.

6.2 Geospatial

Geospatial applications may include the display of a variety of infrastructure items, such as building plans or utility information. Laptops, handsets or wireless data devices could send and receive real-time GIS based location-based data showing active alarms or alerts. Because of the portability of LTE subscriber devices, the technology could be used to determine the location of individual first responders and vehicles or any other mobile asset. The following lists the geospatial applications required by state public safety personnel that involve wireless transmission.

- Automatic Vehicle Location (AVL) for all mobile assets
- In-building and outdoor geospatial positioning of key personnel
- Real-time GPS enabled vehicle tax and HOV lane tolling
- GIS display of CAD events
- GIS display of real-time plowing or salting of road surfaces or road maintenance, closures, etc.
- GIS display of river levels and flooding

The GIS applications are bi-directional. Specifically, some require geospatial information transmissions from field based devices while others relay geospatial information to field units for analysis and decision making.

6.3 Database / Records Management

The following lists the encrypted or secure applications that state agencies either have presently or wish to have remote access to.

- Wireless access to Records Management System
- Wireless access to Bureau of Criminal Apprehension (BCA) databases
- Wireless access to building pre-plans
- Wireless access to building inspections database and/or civil designs

6.4 Security / Encryption Requirements

Law enforcement is required to abide by Federal security standards for their records lookups. This requirement necessitates that the connection be FIPS 140-2 compliant. As a result of FIPS 140-2 requirements, many law enforcement agencies use an encrypted connection to the agency's LAN, also known as Mobile Virtual Private Network (MVPN). The most common MVPN software in use by the participants is from the vendor NetMotion.

HIPPA regulations also require the protection of patient data including the use of wireless biometric vital sign monitoring for patients and key personnel.

In general, most participants indicated that their communication is sensitive in nature and that their transmissions should be encrypted to avoid eavesdropping.

6.5 Other Applications

The variety of wireless data devices continues to expand. The following is a list of potential data applications that state agencies either have presently or wish to have remote access to.

- Wireless internet access and web search
- Wireless access to utility plans database
- Wireless access to weather radar updates
- Wireless access to work order management system
- Wireless access to traffic panels
- Wireless access to email
- Wireless access to other Internet applications

6.6 Web Survey Findings

The following section provides information regarding the application interest of the above mentioned applications as well as other applications. The table below depicts those expressing a need for particular applications:

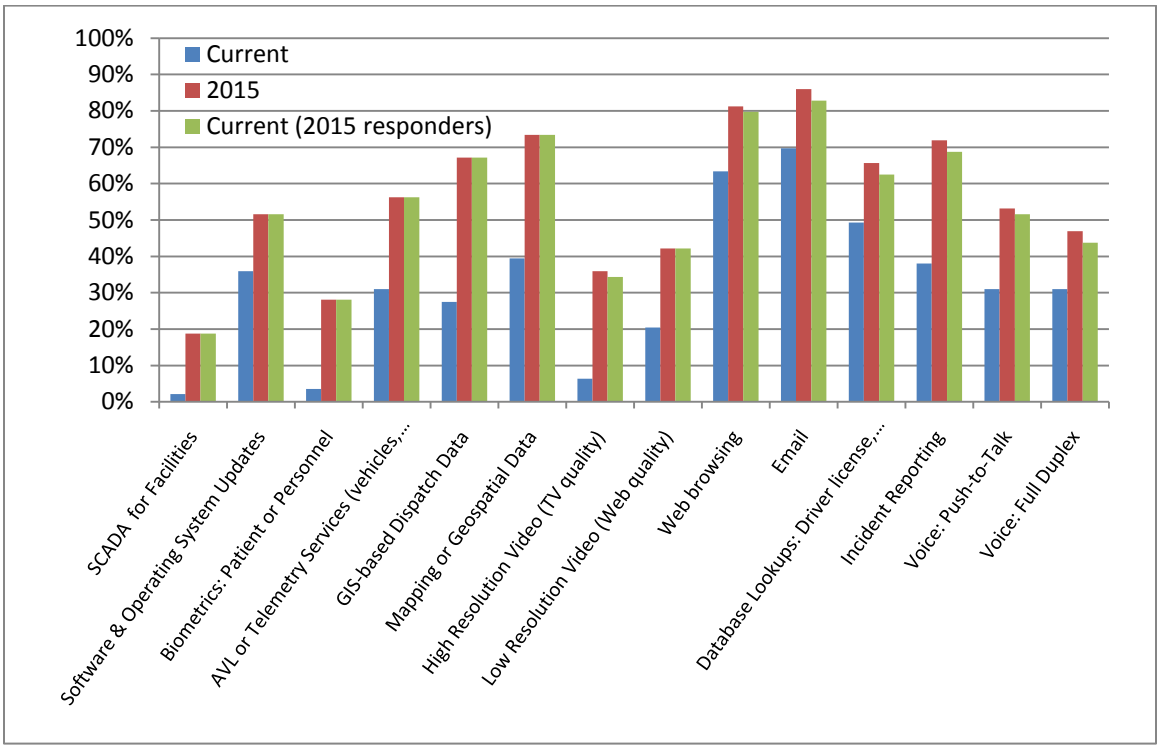


Figure 6: Current and Future Wireless Applications

The graph shows the relative interest in various applications as a percentage of those who currently use, or in 2015 expect use, a particular application. Additionally, the 2015 application question presumed a "new statewide public safety broadband service"[15]. Therefore, the 2015 numbers include both natural growth in anticipated use and the growth that arrives as a result of the new service. The percentages reflect those survey respondents who completed the question (i.e., provided any answer).

The survey depicts that email and web browsing are the most commonly needed applications among the respondents both presently and in 2015. It is important to note that only 64 respondents answered the question regarding 2015 application use, while 142 responded to the current application use. Therefore, comparisons between current and future applications can be biased. As a result, we have included an additional data set. Specifically, looking at the set of respondents that did complete the 2015 information, we have provided the current usage. The data clearly show that there is minimal increase in application use among those who provided information for current and future use. The data also clearly shows that the individuals who did not complete the future question did not use many wireless applications.

Figure 7 provides the quantities of users expected by 2015 on the new service. As opposed to the above chart that shows the percent of respondents that anticipate any use of a particular application, this figure provides a relative comparison of the quantities of users.

[15] The exact question was "How many users for each application would your agency plan to deploy by 2015 if a new statewide public safety broadband service were provided? If unknown, please skip."

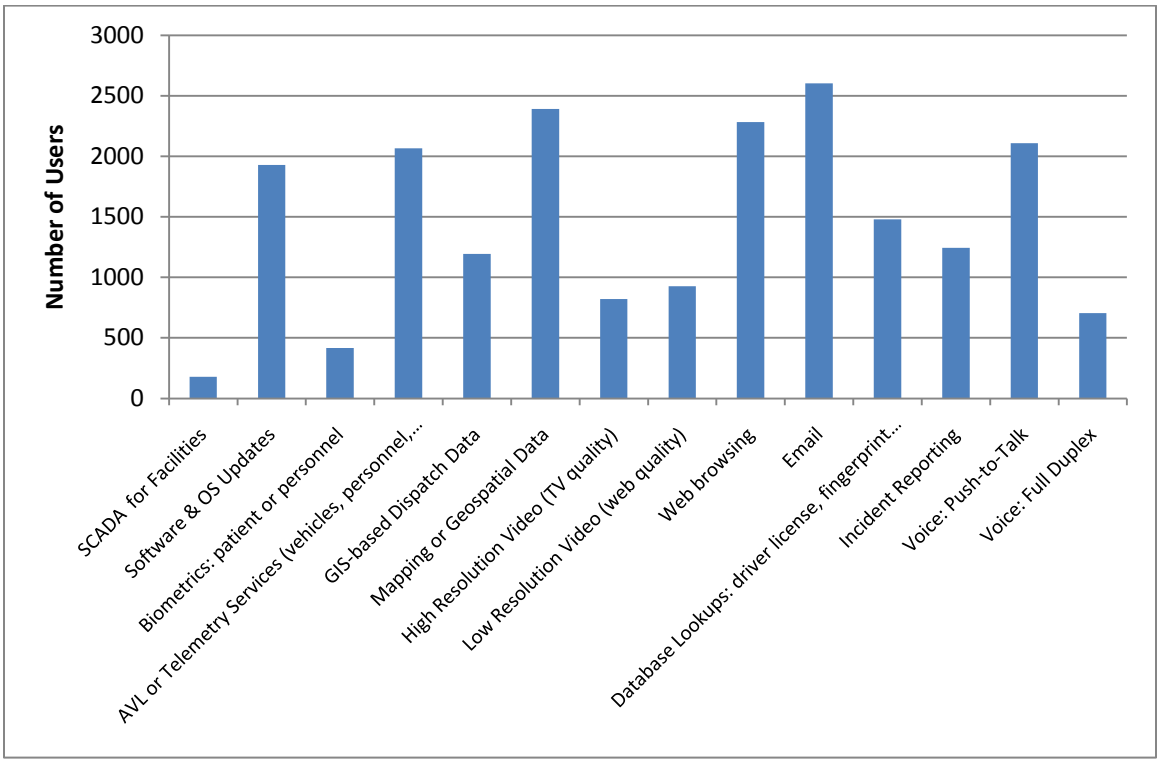


Figure 7: Wireless Applications Users (2015)

The figure shows that email, mapping, web browsing, and push-to-talk are expected to have the most users with over 2,000 users each. Applications such as video, biometrics, and full duplex audio, have less than half as many users as these more common applications. These results are skewed towards the metropolitan areas as their large public safety staffs will dominate these statistics.

7 OTHER USER NEEDS

Other needs that do not neatly fit in to the above categories are found by looking at the existing solutions used by Minnesota public safety agencies. The following chart provides such a view:

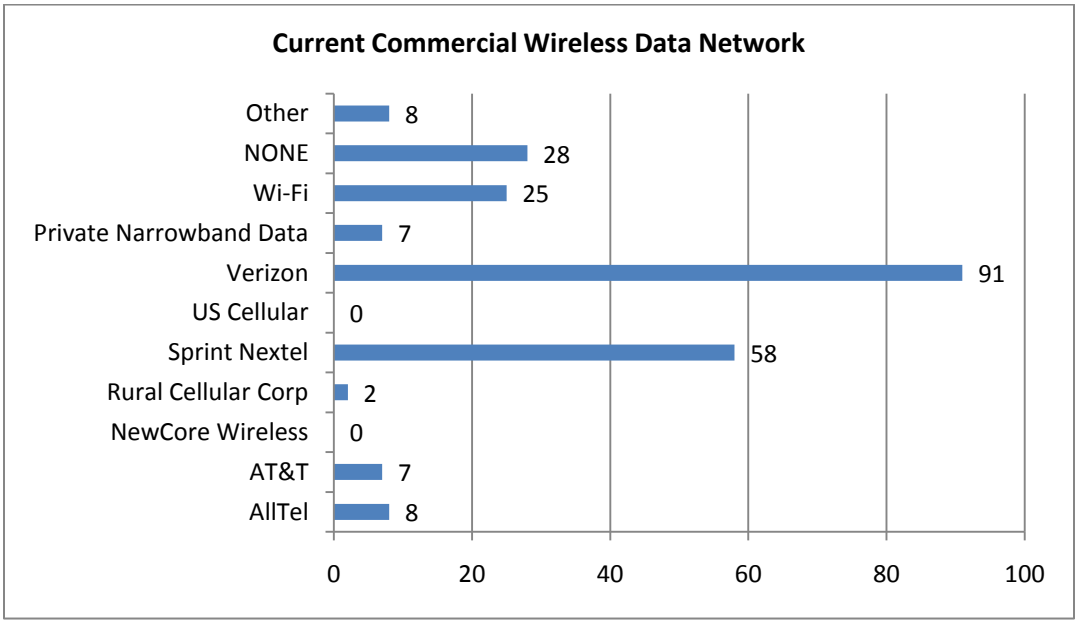


Figure 8: Current Wireless Data System Use

This chart indicates that Verizon and Sprint represent the two largest carriers among respondents[16]. It also indicates that a substantial number of respondents utilize Wi-Fi. Additionally, in the "Other" category, there were multiple responses for private data systems (e.g., VHF and Data Radio). Several respondents indicate a need to integrate these alternate networks with a statewide system.

Additionally, a major communicated user need is affordability. Appendix E contains notable quotations from the web survey regarding the cost expectations for such a service. Several indicate a requirement or expectation that the service would be the same or cheaper cost compared to commercial services.

Several of those interviewed also mention that public safety agencies had trouble affording computers and software. Therefore, while a public safety broadband network is desired, it would provide little value without the access devices and applications that many rural agencies simply cannot afford. While these additional user needs are outside the scope of this project, it is important for the state to consider that this particular project solves only a portion of the overall user needs with regards to public safety broadband communications.

[16] The level of penetration by each operator may be due to the state's existing contractual relationships with these vendors.

8 SUMMARY

This document provides a set of high level user needs regarding a future broadband wireless data solution for the State of Minnesota. There is an interest in a variety of applications for such a solution among state public safety personnel. The web survey respondents accommodated more than 4,000 wireless devices currently and anticipated 6,000 wireless devices by 2015[17]. In total, these needs represent the interests of nearly 200 individuals from the State of Minnesota.

Those surveyed are not unanimous in their requirements. Some had stringent requirements while others are content with lesser requirements. While there are many similarities among the functional, geographic, and types of governments, there are also differences that may have substantial impacts on the viable business models as well as capital and operating costs to achieve the requirements. The following table provides a summary of the requirements as well as the variability among the key requirements. The maximum requirement represents the requirement communicated by those surveyed that which is most difficult to achieve or most limiting. The minimum requirement, on the other hand, represents the requirement which is most easily achieved.

[17] Please note that not all respondents provided information for both current and future devices, and therefore, a direct comparison cannot be made. Only 69 respondents replied to both questions and those responses only make up less than 200 devices. The quantities of 4,000 and 6,000 for current and 2015 devices represent only modems (not the rugged PC and tablet category).

Criteria	Maximum Requirement	Minimum Requirement
Priority	Public safety must be able to pre-empt non-public safety data transmissions	Public safety requires priority over other users but not pre-emption.
Priority Modifications[18]	Public safety must be able to modify user priorities at (or for) an incident in real-time	No respondents stated any other requirement; however we suspect that a "timely" third party adjustment to priority would suffice for some.
Network Availability	Public safety requires 99.999% network availability	Public safety requires cellular grade reliability (99.5%) with increases over time as need arises
Coverage Area	95% coverage on a per county basis	95% coverage of the State; coverage gaps to be decided cooperatively
Coverage In-Building	In-Building portable coverage within 95% of the designated coverage area.	Outdoor or mobile[19] coverage within 95% of the designated coverage area.
Coverage Extension (e.g., COWs)	Portable and high mobile equipment for extending the radio coverage that is owned and controlled by public safety	Agreement with cellular operator to provide augmented coverage within a limited amount of time
Capacity	Sufficient throughput to accommodate a major incident in a metropolitan area and occurring after applications and devices mature	Sufficient throughput to accommodate a major incident in a present-term rural area; 197 kbps on the uplink and 2509 kbps on the downlink
Applications	Real-time streaming high resolution video from an incident scene	Automatic vehicle location
Devices	Commercial roaming capable devices to include smartphones and tablets with embedded modems	USB modems with commercial roaming capabilities
Integration	Devices leverage Wi-Fi and other networks	No alternate network integration required

Table 6: Requirements Summary

[18] The ultimate goal is for the priority of the user to be modified in "real-time", with session persistence (i.e. without interruption of services). At this time there is insufficient information from the vendor community to know whether this is possible within LTE systems. One potential alternative is for the new user priority to be in effect on the next session; thus requiring the user to end, then reinitiate the wireless session.

[19] Use within a vehicle but with an external antenna

The table depicts several substantial differences in need among the users that can have significant impacts on the available business models, deployment costs, and operational costs. The user needs provide the basis for the implementation model and design. As each requirement has a direct impact on the way a network is built and operated, careful consideration should be made to ensure that the benefits are commensurate with the cost.

Thousands of broadband uses, users, devices, and applications are identified in this report that will provide valuable improvements to public safety operations. This assessment clearly shows a substantial need for public safety broadband wireless service that is truly statewide. The services needed by the state public safety personnel are currently not met by existing services, and therefore, the assessment suggests a new, statewide service is required.

9 APPENDIX A – INTERVIEW SCHEDULE AND PARTICIPANTS

Participants	Representing	Meeting Dates
Mark Gieseke	Department of Transportation	01/10/11
John Moreland	Department of Transportation	01/10/11
Paul Weinberger	Department of Transportation	01/10/11
Jakin Knoll	Department of Transportation	01/10/11
Dan Ross	Department of Transportation	01/10/11
Tom Weiner	Department of Transportation	01/10/11
Brian Kary	Department of Transportation	01/10/11
Cory J Johnson	Department of Transportation	01/10/11
Cari Gerlicher	Department of Corrections	01/10/11
Scott Corbo	Department of Corrections	01/10/11
Rick Wyffels	City of Alexandria Police Department	01/10/11
Dave Wright	US Army Corps of Engineers	01/10/11
Teri Alberico	Minnesota National Guard	01/10/11
Jackie Mines	Department Public Safety, Division of Emergency Communication Networks	01/11/11
Ron Whitehead	Department Public Safety, Division of Emergency Communication Networks	01/11/11
Kris Eide	Homeland Security Emergency Management	01/11/11
John Dooley	Homeland Security Emergency Management	01/11/11
Roger Laurence	Hennepin County Sheriff's Office; Metropolitan Emergency Services Board	01/11/11
Brian Askin	Department of Natural Resources	01/11/11
Bob Dahm	Department Public Safety, Fire Marshall	01/11/11
Michael Risvold	City of Wayzata Police Department	01/12/11
Donald Cheung	Bureau of Criminal Apprehension	01/12/11

Participants	Representing	Meeting Dates
Kurt Augustin	Bureau of Criminal Apprehension	01/12/11
Bob Johnson	Bureau of Criminal Apprehension	01/12/11
Micah Myers	City of St. Cloud; Central Minnesota RAC	01/13/11
Troy Langlie	Grant County Sheriff's Office	01/13/11
Mark Dunaski	Minnesota State Patrol	01/13/11
Steven Bluml	Minnesota State Patrol	01/13/11
Pat Novacek	Northwest Minnesota RAC	01/14/11
Pat Coughlin	Department of Natural Resources; Minnesota Interagency Fire Center (MIFC)	01/14/11
Darlene Pankonie	Washington County PSAP; Next Generation NG911 Advisory Committee	01/14/11
Russ Reilly	Office of Enterprise Technology	01/14/11
Mark M. Nelson	Office of Enterprise Technology	01/14/11
Ullas H Kamath	Office of Enterprise Technology	01/14/11
Monte Fronk	Mille Lacs Band of Ojibwe, Department Public Safety	01/25/11
Reed Anderson	US National Park Service, Midwest Regional Office	01/25/11
Joe Snyder	US National Park Service, Midwest Regional Office	01/25/11
Troy Tretter	Minnesota National Guard	01/25/11
Lou Mosely	Minnesota National Guard	01/25/11
Chris Kummer	Hennepin County Emergency Medical Services	01/26/11
Wayne Kewitsch	City of Richfield, Fire Department	02/01/11

10 APPENDIX B – DETAILED INCIDENT CAPACITY ANALYSIS

The purpose of the incident-based review is to understand the wireless data requirements of the responding agencies for a specific incident that has substantial demand on a wireless network. The primary objective is to identify the aggregate throughput needed for the incident. The incident-based review is to capture:

- Timing of wireless data use
- Type & configuration of application or type of data
- Number of users for each application
- Location of users

10.1 Incident Description

The scenario for the incident is as follows:

- On a typical mid-January day a storm bears down on the state of Minnesota. Heavy snowfalls are reported followed by strong winds. The temperatures vary throughout the day as snow turns to freezing ice then back to snow.
- At 12:30 PM an unidentified male enters a High School building (~2,000 students) and begins to open fire with a small caliber weapon. There are approximately 10 casualties ranging from the critically injured to minor wounds.
- The individual then breaks into an occupied classroom and proceeds to take hostages.
- The first officer arrives on scene to find the individual barricaded within the classroom along with the hostages.

10.2 Incident Organization

Timeline of key components of the incident are as follows

- First Law Enforcement Officers (Incident Commander and Task Force) on scene (within 3-5 minutes)
- Strike Team arrives (Time = 10 to 30 minutes)
- Fire and EMS Units sent to staging area (Time = 10 to 30 minutes)
- Incident Commander arrives and the Unified Command is declared and setup (Time = 3 to 30 minutes)
    - COML setup

- Intelligence Unit arrives
- Technical Specialists arrive
- Planning Section is setup

- Inner and Outer Perimeters are secured, Staging Area Operations Section and Logistics Section is setup; concurrently with the IC (Time = 30 minutes)
  - Triage of victims and removal to Staging Area
  - Evacuation of non-responder personnel within Inner and Outer Perimeters
  - Questioning of witnesses
- Strike teams (SWAT) deploy, at least four teams, four officers per team (Time =60 minutes)
  - Deployment of remote monitoring devices
  - SWAT teams to conduct room-by-room clear and secure up until reaching the immediate incident area (Time = 120 minutes)
  - "Throw phone" given to Offender (Time = 120 minutes)
  - Negotiations
- Interdiction (Time = 180 minutes)
  - Offender is subdued
- Incident area is fully secured (Time = 185 minutes)
  - Any remaining victims are treated
  - Statements from witnesses are gathered
- Incident Closed out (Time = 245)

The ICS organizational chart for all personnel present at the incident is located below.

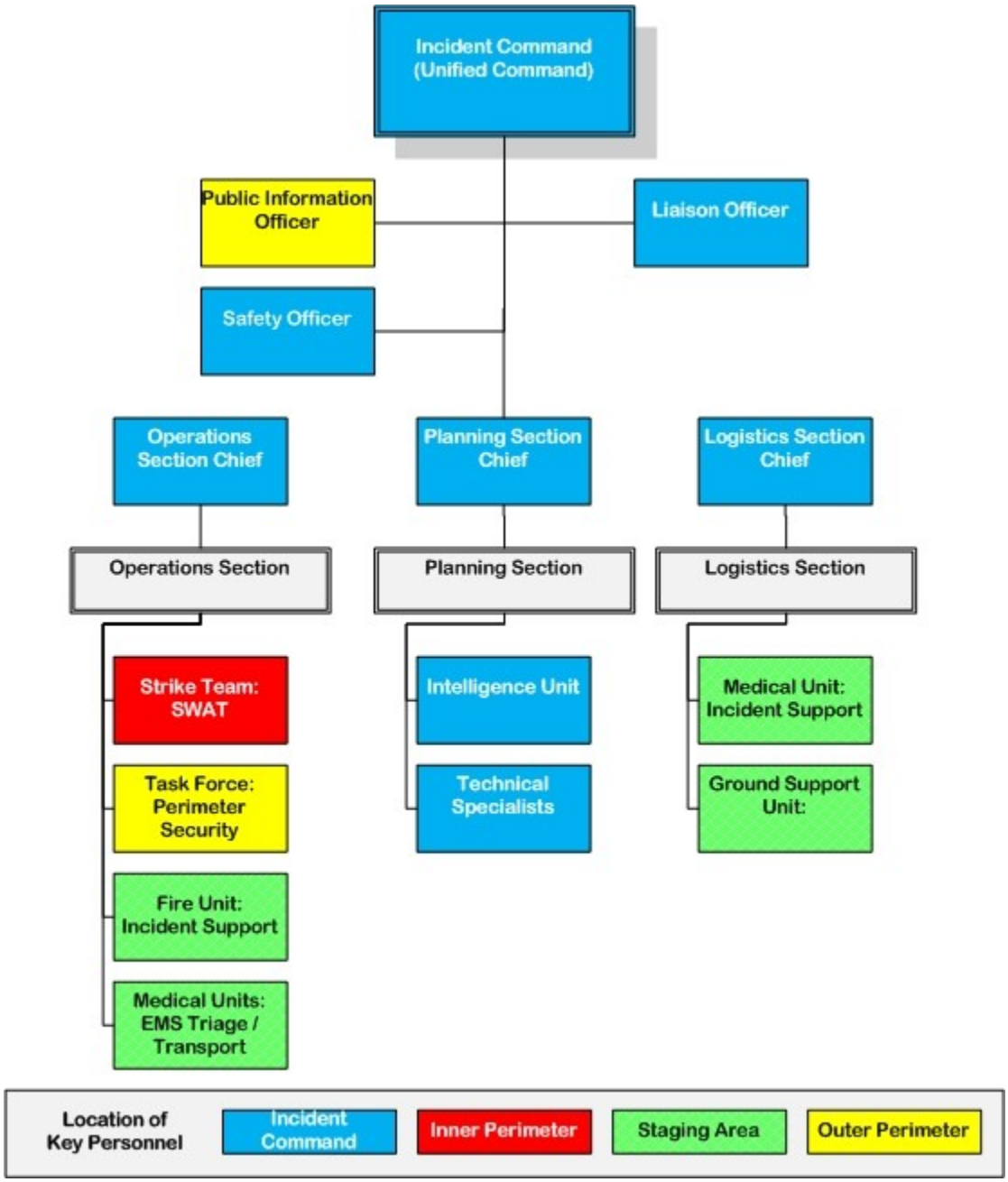


Figure 9: ICS Organization Chart of the Incident

10.2.1 Incident Response Teams and Location of Key Personnel

The incident response team will consist of many disciplines. The estimated number of responders per team as well the buildup over time is as follows:

10.2.1.1 Task Force: up to 68

The Task Force Contingent will be responsible for the security of the inner and outer perimeters and crowd control. The estimation assumes up to 12 roadblocks and 4 officers per roadblock. The remaining 20 officers will be used as patrols, reliefs and crowd control. The Task Force Contingent will also monitor, manage and control the Evacuation Area and will provide briefings to the press as warranted. Task Force is responsible for the control of access to areas within the outer perimeter. Depending on the duration of the incident, the Incident Commander may schedule reliefs.

10.2.1.2 Incident Command / Unified Command: up to 12

The Unified Command Contingent will grow up to 12, and will consist of the Incident Commander, Liaison Officer, Operations Section Chief, Planning Section Chief Logistics Chief Safety Officer and members of the Planning Section: the Intelligent Team (three total) and Technical Specialists.

10.2.1.3 Strike Team: up to 16

The Strike Team Contingent is made up of a minimum of four teams of four SWAT officers each.

10.2.1.4 Operations Section:

The remaining member of the Operations Section will consist of the Fire and Medical Unites. The Fire Contingent consists of two engines (three responders per engine) EMS Contingent consists of three ambulances with two EMTs per ambulance. The Fire and EMS Units will remain at the Staging Area until as directed by the Operations Section Chief.

10.2.1.5 Logistics Section:

The Logistics Section will consist of additional Medical Units for Incident Support and Ground Support Units. They will be located at the Staging Area and will be managed by the Logistics Section Chief.

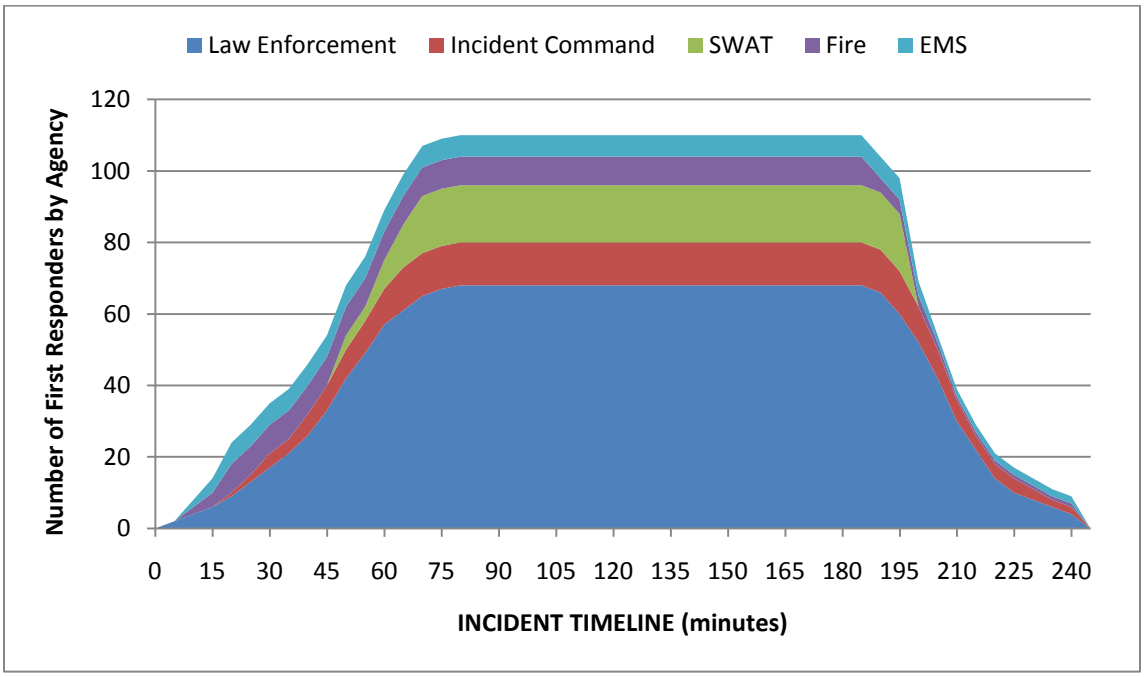


Figure 10: Incident Timeline vs. the Buildup of Resources

The figure shows the buildup of first responders over the incident timeline. It is expected that there will be a substantial public safety presence within 30 minutes in the vicinity. The figure also shows that the peak personnel on scene, which is correlated with the peak wireless data usage, occurs at Time = 75 minutes. However, it is important to note that almost half of the on-site first responders will not use a significant amount of wireless data services. The details regarding the specific wireless communication requirements for the incident responders are provided later in the section.

10.2.2 Incident Response Team for a Rural Area

The rural response often will be limited to the reduced quantity of responders who could render aid in a timely manner. In this scenario, the incident personnel will be made up of the following:

10.2.2.1 Task Force / Strike Team (SWAT): up to 8

The Task Force Contingent will be responsible for the interdiction and security of the inner and outer perimeters. The estimation assumes up to two (2) roadblocks, single officer per roadblock. The remaining six (6) officers will make up the Strike Team (SWAT) as soon as the team is constituted in sufficient number.

10.2.2.2 Incident Command: 1

The Incident Command will consist of a single officer.

10.2.2.3 Operations and Logistics Sections: up to 10

The Operations and Logistics Sections will consist of a Fire Contingent of two engines (three responders per engine) and an EMS Contingent consisting of two (2) ambulances with two EMTs per ambulance.

10.3 Incident Area

The Incident area is broken into two separate parts; the Inner Perimeter and Outer Perimeter. The Inner Perimeter is roughly 640 feet tall by 950 feet across encompassing an area of approximately 608,000 square feet. The Outer Perimeter is a polygon covering an area of 14.5 million square feet or an area of a little more than one half square mile.

Figure 11: Plan View of Incident Area

The area over which the incident occurs has substantial impact on how a wireless network can accommodate the demand. The less dense the usage, the easier it is for a wireless network to accommodate the demand. The reverse is also true. Specifically, a very high density of users with substantial demands is more difficult to accommodate. In addition, a wireless network provides variable performance as the distance from the "cell site" changes. It is for this reason that the demand requirements are divided into four (4) key areas; Strike Team (SWAT) (Inner Perimeter), Incident

Command/Unified Command, Staging Area and Outer Perimeter/Evacuation Area. The Extraction Area is assumed to generate a minimal load on the network.

10.4 General Assumptions

The following key assumptions were made in assessing the overall demand for the incident:

- We assume for the purposes of demand on the data network that all voice services are run over separate networks (i.e., they do not place their "loads" on this wireless data network). For push-to-talk, we assume that traffic is carried over the ARMER network. Except where otherwise noted, we assume that cell phone style voice traffic is carried by the commercial cellular networks.

- We have assumed that there is no other traffic other than that which is generated by the incident.

- We assume all video cameras streaming data over the wireless data network are using efficient video codecs (H.264)

- We assume an efficient video management architecture. Specifically, if the same uplink (user in the field to cell site) video stream is viewed by multiple parties in the field, it does not require multiple uplink streams to support. In addition, we assume that the uploaded video is broadcasted to multiple incident commanders. In other words, if five users are viewing the same video in the area, the video is transmitted only once on the downlink (cell site to user in the field)

- Updates of vehicular telemetry (Automatic Vehicle Location) occur every 60 seconds. Telemetry for the SWAT Team is on a per second basis.

- Biometric readings will not be sent unless if triggered by an alarm; then in which case the data will be streaming. For this incident, we have assumed three EMS biometric devices in alarm.

- The video generated by the SWAT Team and coming from the inner perimeter is destined for the Incident Command and fixed locations (e.g., an EOC). In other words, the video generated at the incident scene must be transported to a fixed network outside the outer perimeter.

10.5 Wireless Data Requirements

The wireless data requirements are broken into three separate groups; Incident Command/Unified Command, Strike Team (SWAT) and Task Force (Perimeter Security). The wireless data requirements of the Strike Teams and the Unified Command are expected to be considerable, whereas the Perimeter Security will be minimal and mostly reliant on the push-to-talk communications, and therefore, the ARMER Network.

For each location, in the sections below, we provide a description of the applications requiring data communications (i.e., applications that are resident on the computers at the scene but do not require wireless communication are not listed). Following the written descriptions, we provide tables

representing the net demand placed on a wireless network (or networks) at that location. The tables provide the peak instantaneous demand from the application as well as average demand. The difference applies to "bursty" applications that are not constantly transmitting. For these applications, such as web browsing and file download, high quality of service is defined by receipt of the data within a limited timeframe (e.g., five seconds). However, it is unlikely that all "bursty" applications would require bandwidth simultaneously, and therefore, we show their average demand as well as the peak demand.

10.5.1 Strike Teams (SWAT) - Inner Perimeter

There are four SWAT teams of four officers each. The functional requirements for each team's equipment are listed as follows:

1. Helmet or Lapel camera. Assumes:
    a. Streaming video QCIF resolution[20] at 12 frames per seconds[21] (fps) as a default to provide some level of situational awareness from each SWAT Team member[22].
2. Tactical Telemetry / In-Building Geo-Positioning and Tracking[23]. Assumes:
    a. Per second updates to position location
3. Biometric monitoring of vital signs. Assumes:
    a. Streaming data only upon an alert or query
4. Fixed situational awareness cameras brought by the SWAT Team; can be a robotic device, a pole camera or a portable staged camera tacked to a wall (one device per SWAT team). Assumes:
    a. One camera streaming at a "high" resolution (4CIF at 24fps)
5. Fixed situational awareness cameras brought by the SWAT Team; can be a robotic device, a pole camera or a portable staged camera tacked to a wall (one device per SWAT team)
    a. Assumes three cameras streaming at a "low" resolution (QCIF at 24fps)
6. "Throw Phone" – Voice Communications. Assumes:
    a. Voice communications from Throw Phone to Negotiator
7. "Throw phone" – Discrete Video. Assumes:
    a. Transmission of discrete video to Incident Command

[20] Please see Appendix A for a description of video resolution.

[21] The "frame rate" or frames per second describes the number of images that appear every second. The higher the frame rate, the more fluid the motion appears. A frame rate of 24 fps appears to be full motion to the human eye. A frame rate of 12 will appear slightly "choppy" where the motion is less fluid.

[22] The incident commander will have the option to increase the video quality of any of these streams as needed. We assume that when this occurs, one of the other streams from fixed locations (described below) is reduced to this lower quality. Ultimately, the total number of video streams from the incident represents a "budget" that the Incident Commander would have available to use as necessary.

[23] We recognize that in-building geopositioning is a challenge. We assume that the network or some other means to geo-locate is available and that the wireless data network must transmit the position information from inside the building.

The following Table displays the aggregated data requirements for the Strike Team Location within the Inner Perimeter:

	Description	Application Type	Units	Activiity	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
	Strike Team Data Services							
1	Helmet/Lapel camera video upload from SWAT Team to Unified Command via central media server	Video - Low Res Uplink	16	100%	598 kbps	192 kbps	598 kbps	192 kbps
2	Tactical Telemetry (geo-positioning) upload from SWAT Team to central data	Telemetry - Tactical	16	100%	11 kbps	1 kbps	11 kbps	1 kbps
3	Biometrics (monitoring only when in alarm)	Biometrics	16	10%	192 kbps	192 kbps	19 kbps	19 kbps
4	Fixed Situation Awareness Cameras along perimeter (deployed camera)	Video - High Res Uplink	1	100%	1014 kbps	16 kbps	1014 kbps	16 kbps
5	Fixed Situation Awareness Cameras along perimeter (deployed cameras)	Video - Medium Res Uplink	3	100%	760 kbps	48 kbps	760 kbps	48 kbps
6	Throw Phone - Voice communications between Assailant & Negotiator	Voice over LTE	1	40%	27 kbps	27 kbps	11 kbps	11 kbps
7	Throw Phone - Discrete video	Video - Medium Res Uplink	1	100%	253 kbps	16 kbps	253 kbps	16 kbps
		Strike Team Subtotal:			**2856 kbps**	**492 kbps**	**2667 kbps**	**303 kbps**

Table 7: Strike Team Data Requirements

10.5.2 Incident Command / Unified Command

The Unified Command will require wireless data access to the following data sources:

1. Internet Web Browsing: Intelligence Team web-based research in support of the incident. Assumes:
    a. Up to two computers actively pulling data up to 17% of the time off of typical web pages.
2. Internet Web Browsing: Intelligence Team web-based research in support of the incident. Assumes:
    a. Up to two computers actively pulling data 26% of the time off of *graphics rich* web pages that can include web-based incident management software such as WebEOC.
3. Encrypted access to Records Management System and Bureau of Criminal Apprehension data bases. Assumes:
    a. Up to five computers actively requesting or writing up to 50 instances of data; approximately 4.3% of the time.
4. Download of Satellite Images or Maps. Assumes:
    a. Up to two computers actively requesting data within a five minute window of peak demand.
5. Pre-Plans, Building Plans and Utility Layers. Assumes:
    a. Building drawings including utility and HAZMAT information is transferred to two or more Section Chiefs; Peak Demand assumes a total of two requests of 10MB each within a 30 second window. Average Demand assumes a total of ten requests of 10MB each within a ten minute window.

6. Incident Management Software Updates. Assumes:
    a. Up to four computers (each key liaison or mutual aid agencies) actively pulling data 100% of the time.
    b. Telemetry Updates from AVL tracking of public safety vehicles and assets every 15 seconds.
7. Video Conferencing between Unified Command / EOC/ Staging Area. Assumes
    a. One instance at the Incident Command location; note: an additional instance may be required if SWAT Team Operations Section Chief is not located at the Unified Command location.
8. "Throw Phone" – Voice Communications. Assumes:
    a. Voice communications from Throw Phone to Negotiator at the Unified Command
9. "Throw phone" – Discrete Video. Assumes
    a. Transmission of discrete video to Unified Command
10. Fixed Situational Awareness Camera – Deployed Cameras. Assumes:
    a. One high resolution video from staged camera sources.
11. Fixed Situational Awareness Cameras – Deployed Cameras. Assumes:
    a. Three low resolution video from staged camera sources.
12. School Camera. Assumes:
    a. One high resolution in-building video from school's video management server.
13. School Cameras. Assumes:
    a. Four low resolution in-building video from school's video management server.
14. Traffic or Street Cameras. Assumes:
    a. Four low resolution video streams of near-by Traffic or Street cameras.
15. Helicopter Video. Assumes
    a. One high resolution video of the incident area. We assume that it is transported to the fixed network using other non-terrestrial networks[24], and therefore, only the downlink to IC is represented in the scenario.
16. SWAT Team Video. Assumes:
    a. Sixteen low resolution matrix views coming from the SWAT teams.
17. NG911 Video:
    a. Next Generation 911 video clips received by PSAP from the general public and then sent to Incident Commander.

[24] Airborne operations are problematic for terrestrial cellular based networks. Therefore, we have assumed that this traffic is carried over alternate links. This could include microwave licenses or 4.9 GHz spectrum.

The following Table displays the aggregated data requirements for the Incident Command Location:

	Description	Application Type	Units	Activiity	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
	Unified Command Data Services							
1	Intelligence Team: Web browsing (30 pg hits / hour)	Web Browsing - Basic	2	17%	32 kbps	256 kbps	5 kbps	43 kbps
2	Intelligence Team: Web browsing (30 pg hits / hour)	Web Browsing - Graphics Rich	2	26%	32 kbps	256 kbps	8 kbps	67 kbps
3	Unified Command access to their RMS and BCA databases (50 read/write per hour max)	Data transfer med - 128kB/s	5	4.3%	640 kbps	640 kbps	28 kbps	28 kbps
4	Download of overhead satellite images	GIS - Maps Satellite Images	2	21%	0.2 kbps	512 kbps	0.03 kbps	107 kbps
5	Preplans, Building Plans & Utility Layers (10MB)	Image Transfer - High Resolution	2	100%	0.1 kbps	2731 kbps	0.1 kbps	683 kbps
6	Incident Management Software with CAD and Telemetry updates (server-based)	CAD, Telemetry & Command Board	1	100%	40 kbps	128 kbps	40 kbps	128 kbps
7	Video/Audio Video Conferencing between Incident Command & EOC	Video Conferencing	1	100%	63 kbps	253 kbps	63 kbps	253 kbps
8	Throw Phone - Voice communications between Assailant & Negotiator	Voice over LTE	1	40%	27 kbps	27 kbps	11 kbps	11 kbps
9	Throw Phone - Discrete video	Video - Medium Res Downlink	1	100%	16 kbps	253 kbps	16 kbps	253 kbps
10	Fixed Situational Awareness Camera (deployed camera)	Video - High Res Downlink	1	100%	16 kbps	1014 kbps	16 kbps	1014 kbps
11	Fixed Situational Awareness Camera (deployed cameras)	Video - Medium Res Downlink	3	100%	48 kbps	760 kbps	48 kbps	760 kbps
12	School Camera: accessed via the school's video management server	Video - High Res Downlink	1	100%	16 kbps	1014 kbps	16 kbps	1014 kbps
13	School Camera: accessed via the school's video management server	Video - Low Res Downlink	4	100%	64 kbps	150 kbps	64 kbps	150 kbps
14	Traffic or Street Cameras	Video - Low Res Downlink	4	100%	64 kbps	150 kbps	64 kbps	150 kbps
15	Helicopter Camera Video: High resolution matrix view of video downloaded to Incident Command	Video - High Res Downlink	1	100%	16 kbps	1014 kbps	16 kbps	1014 kbps
16	Strike Team Video: viewed by the Tactical Team Commander	Video - Low Res Downlink	16	100%	16 kbps	598 kbps	16 kbps	598 kbps
17	Video from NG911	Video - Medium Res Downlink	1	100%	16 kbps	253 kbps	16 kbps	253 kbps
		Unified Command Subtotal:			**1106 kbps**	**10009 kbps**	**427 kbps**	**6524 kbps**

Table 8: Unified Command Data Requirements

10.5.3 Staging Area

The Staging Area will consist of the remaining responding elements that for reasons of space, safety or practicality will require a separate aggregation point more removed from the incident center. Specifically, the staging area will consist of the remaining units from the Operations Section (Fire and Medical Units) and all units assigned to the Logistics Section. The supporting agencies will provide the

logistics in support of the incident. The Logistics Section Chief will command the Ground Support Units from DOT and/or Public Works who will be responsible for clearing roads and the setting up of barriers.

1. Telemetry Updates from AVL Tracking. Assumes:
    a. The upload or reporting of all public safety vehicles and assets.
2. Video Conferencing with White-Boarding. Assumes:
    a. One instance of low resolution video
3. Incident Management Software Updates. Assumes:
    a. One computer actively pulling data 100% of the time.
    b. Telemetry Updates from AVL tracking of public safety vehicles and assets every 15 seconds.
4. Encrypted access to Records Management System and Bureau of Criminal Apprehension data bases. Assumes:
    a. Up to three computers actively pushing and pulling data 33% of the time.
5. Patient Biometric Monitoring of vital signs Assumes:
    a. Three critical-care patients being treated[25].
6. EMS Video Feeds for medical surveillance. Assumes:
    a. Three EMS units being backhauled to a Trauma Care Physician at medium resolution.
7. Replication of Incident Command Video sources; (not listed below). Assumes:
    a. All video that is sent to Unified Command from the Inner Perimeter is available to the staging area via multicast/broadcast. Therefore, no additional bandwidth is consumed for the video needs of the staging area.

The following Table displays the aggregated data requirements for the Staging Area Location:

	Description	Application Type	Units	Activiity	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
	Staging Area Data Services							
1	AVL Reporting on Physical Assets at Staging Area (vehicles)	Telemetry	10	25%	0 kbps	0 kbps	0 kbps	0 kbps
2	Video/Audio Video Conferencing	Video Conferencing	1	100%	63 kbps	253 kbps	63 kbps	253 kbps
3	Incident Management Software with CAD and Telemetry updates (server-based)	CAD, Telemetry & Command Board	1	100%	40 kbps	128 kbps	40 kbps	128 kbps
4	General access to the RMS Systems	Data transfer med - 124kB/s	3	33%	144 kbps	144 kbps	48 kbps	48 kbps
5	Patient Biometrics the EMS Unit to the Trauma Care Physician	Biometrics & Positioning	3	100%	36 kbps	36 kbps	36 kbps	36 kbps
6	Video from the EMS Unit to the Trauma Care Physician	Video - Medium Res Uplink	3	100%	760 kbps	48 kbps	760 kbps	48 kbps
		Staging Area Subtotal:			**1044 kbps**	**609 kbps**	**947 kbps**	**513 kbps**

Table 9: Staging Area Data Requirements

[25] Considering the great importance by EMS on the biometric monitoring and the usefulness of streaming video from the scene to a trauma care physician as well as the potential for a violent outcome, it was assumed that there should be an allowance built into the system to support a minimum of three critical care patients.

10.5.4 Perimeter Requirements

The perimeter is defined as the area at the outer edges of the incident as well as other incident related traffic that is not specifically within the incident area. The following represents the perimeter traffic:

1. AVL from Law Enforcement Assets at the Perimeter. Assumes:
    a. Telemetry Updates from AVL tracking of public safety vehicles and assets every 15 seconds.
2. Average System Load per the following items, at a minimum:
    a. EMS Traffic En Route: While patients are in transit to hospitals, we presume that the EMS units are sending video, biometrics data and AVL tracking information to hospitals.
    b. DOT: Transportation officials outside the incident perimeter are involved in various incident related AVL activities.
    c. Road Treatment Activities: Snow plow AVL tracking; potentially two plows in the vicinity keeping roads clear for emergency vehicles.
    d. Temporary Signs: Placement of temporary road signs diverting vehicular traffic with communications to the signs as necessary.

The following Table displays the aggregated data requirements for the area at and outside the Outer Perimeter:

	Description	Application Type	Units	Activity	PEAK Uplink	PEAK Downlink	Average Uplink	Average Downlink
	Perimeter Data Services							
1	AVL Reporting on Physical Assets around Perimeter (2 patrol cars per roadblock, 12 roadblocks + 10 misc.)	Telemetry	34	25%	1 kbps	0 kbps	1 kbps	0 kbps
2	Average System Load on the Sector	Data transfer med - 128kB/s	2	100%	256 kbps	256 kbps	256 kbps	256 kbps
				Perimeter Subtotal:	**257 kbps**	**256 kbps**	**257 kbps**	**256 kbps**

Table 10: Perimeter Data Requirements

10.6 Incident Requirements Summary

The active shooter incident presents a significant amount of demand on wireless networks. The majority of the traffic is concentrated in one small area encompassing 0.52 square miles. Although the coverage area is small, it is feasible that the three primary incident areas could be served by different cell sites or different sectors.

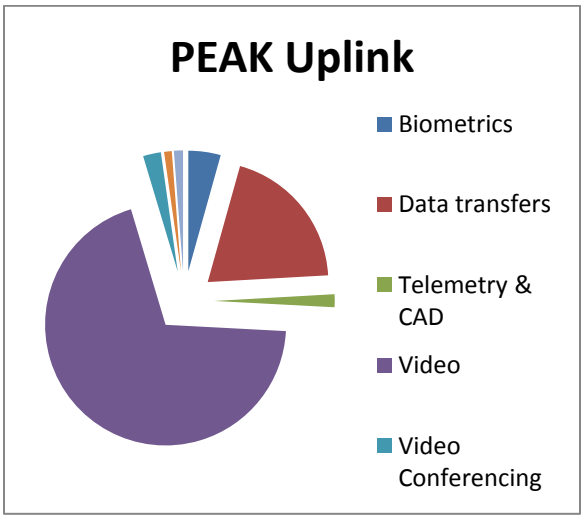
In total, the Incident requires an average downlink capacity of 7,596 kbps and a potential PEAK capacity demand of 11,366 kbps. On the uplink it will require an average of 4,298 kbps with a potential PEAK capacity demand of 5,263 kbps. The table below presents the aggregate findings of the above sections.

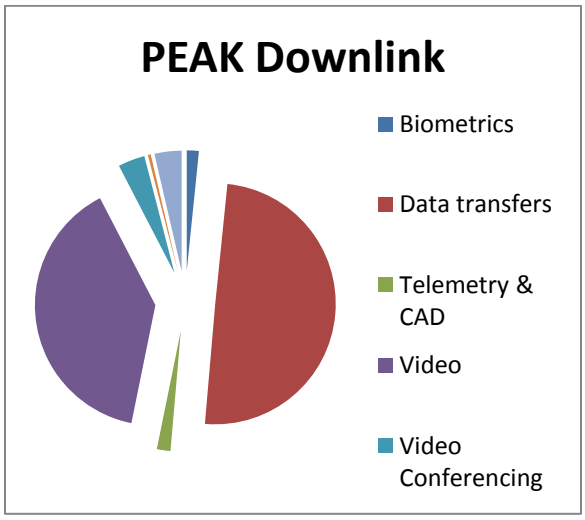
	PEAK Uplink	PEAK Downlink	Average Uplink	Uplink %	Average Downlink	Downlink %
Strike Team Subtotal:	2856 kbps	492 kbps	2667 kbps	62%	303 kbps	4.0%
Unified Command Subtotal:	1106 kbps	10009 kbps	427 kbps	10%	6524 kbps	86%
Staging Area Subtotal:	1044 kbps	609 kbps	947 kbps	22%	513 kbps	7%
Perimeter Subtotal:	257 kbps	256 kbps	257 kbps	6%	256 kbps	3.4%
INCIDENT TOTALS:	**5263 kbps**	**11366 kbps**	**4298 kbps**		**7596 kbps**	

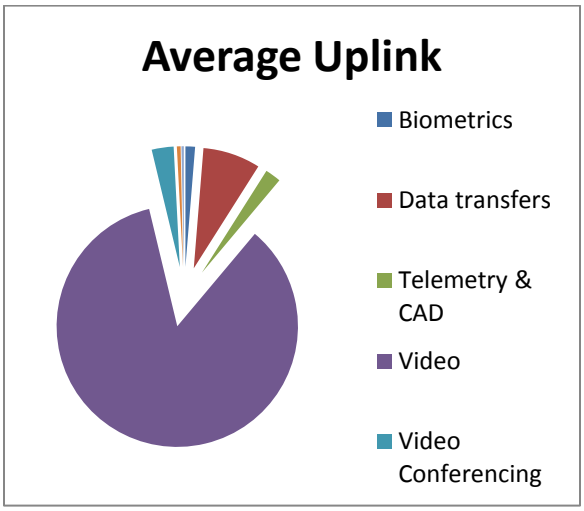
Table 11 - Summary of Incident Data Requirements

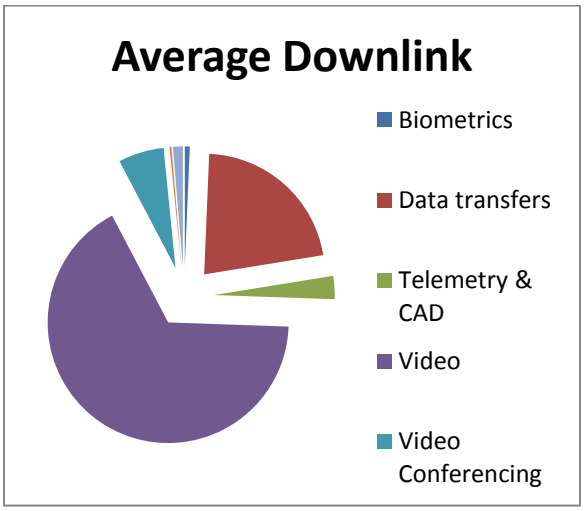
Of the total average downlink traffic (7,596 kbps), 5,206 kbps of the downlink total would be multicasted or broadcasted throughout the service area, requiring only one feed. If not, each recipient of a video stream would receive a separate stream on the downlink. To support the multicast scenario, we have assumed a client-server architecture on the uplink video requiring only one uplink stream. If such an architecture does not exist, the uplink and downlink video would be multiplied for every viewer of that video.

The incident underscores a number of important applications that will be essential to future public safety operations. The following charts list those application categories as per their usage percentage:






Average Uplink
Biometrics
Data transfers
Telemetry & CAD
Video
Video Conferencing


Average Downlink
Biometrics
Data transfers
Telemetry & CAD
Video
Video Conferencing

11 APPENDIX C – VIDEO RESOLUTION COMPARISONS

The video resolution is based upon the number of vertical and horizontal pixels that are being encoded. The incident is using three specific resolutions for various camera views, QCIF (or Quarter-CIF), CIF and 4CIF. The following images provides as example of the degradation of quality between the three resolutions.

Figure 12: Comparison of Resolution

Figure 13: Detailed Comparison of Different Resolutions[26]

The detailed figures show that the man in the window would not be clearly recognizable as a man in the QCIF resolution, becomes somewhat recognizable at CIF resolution, and becomes more clearly recognized as a man in the 4CIF resolution. However, overall, the QCIF image does provide overall situational awareness. Because there are significant differences between transmission speeds of the various resolutions, the requirements assume, in each case, the minimum necessary resolution (and frame rate) to meet the operational needs of the incident. Because each video source is constantly transmitted in this incident scenario, those reviewing the video (i.e., the incident commander or intelligence officers) would have the dynamic ability to increase the resolution and frame rate, on the desired video streams in real time.

[26] This image was take at a focal length (distance to object) of approximately 185 feet. The focal length will have a direct impact on the ability to discern specific objects at a given resolution. One should consider the resolution in tandem with the expected viewing distance (focal length) when defining the codec and frame rate.

12 APPENDIX D – WEB SURVEY QUESTIONS

This survey is designed to assess and estimate Minnesota's present and future wireless broadband data requirements. This survey is part of a project to determine the technical and operational requirements for a potential future public safety wireless broadband data network for first responders and other public safety officials in the state of Minnesota. This survey is being conducted on behalf of the Minnesota Department of Public Safety. Please note that the existence of this survey does not indicate that the state of Minnesota necessarily plans to build such a network.

For further information on the "Minnesota Public Safety Wireless Broadband Data Network Requirements Project" please contact:

Brandon Abley

Brandon.Abley@state.mn.us

Technical Coordinator

Minnesota Emergency Communication Networks

445 Minnesota Street, Suite 137

St Paul, Minnesota 55101-5137

Office: (651) 201-7554

Cell: (651) 263-0002

Contact Information

Please provide your contact information. This information is needed to validate your response and enable us to follow up if we have additional questions.

Name: _____

Agency: _____

City/Town: _____

ZIP: _____

Email Address: _____

Phone Number: _____

Please indicate the affiliation of your agency

- State Government
- County Government
- City Government
- Tribal Government
- NGO
- Hospital
- Other (please specify):

Please indicate the category that best describes your agency

- Law Enforcement
- Fire
- EMS
- Emergency Management
- Other Public Safety
- Local/Municipal/City/County
- Federal Government
- Tribal Government
- Non-Governmental Organization
- Other

Emergency Support Functions

Please indicate the public safety and public service functions your agency represents. Please check all that apply.

- ESF 1-Transportation
- ESF 2-Communications
- ESF 3-Public Works
- ESF 4-Firefighting
- ESF 5-Information and Planning
- ESF 6-Mass Care
- ESF 7-Resource Support
- ESF 8-Health, Medical, and EMS
- ESF 9-Search and Rescue
- ESF 10-Hazardous Materials
- ESF 11-Food and Water
- ESF 12-Energy
- ESF 13-Military Support
- ESF 14-Public Information
- ESF 15-Volunteers and Donations
- ESF 16-Law Enforcement
- ESF 17-Animal Services
- Public Service (weights and measures, inspectors, etc.)
- Education/Schools
- Sanitation & Sewer
- Other (Please Specify)

Current Wireless Service

Are you currently using a commercial or private wireless data network or cellular air card to conduct business? Check all that apply.

- AllTel
- AT&T
- NewCore Wireless
- Rural Cellular Corporation (RCC)
- Sprint Nextel
- US Cellular
- Verizon
- Narrowband Data (Private)
- Wi-Fi
- NONE

other (please specify)

Please describe areas where your users have experienced coverage problems on the existing wireless network. If you'd like, you can fax a map to Mark Navolio at 703-992-6583 indicating the poor coverage area(s) or you can email mnavolio@televate.com. Please provide your name and the network information on the map.

Wireless Network Details

If applicable, please indicate the details of the wireless system you operate. For example, please provide the number of sites/APs, technology (e.g., Wi-Fi) and RF spectrum used (VHF, UHF, 900 MHz, 2.4 GHz, etc.).

Subscriber Devices

What device(s) do you currently use on the existing wireless network(s)? Check all that apply.

- ☐ Smartphone or PDA
- ☐ Rugged Smartphone or PDA
- ☐ Embedded Cards (modem embedded inside computer)
- ☐ Expansion Slot or USB Modem
- ☐ Express Card
- ☐ USB Modem Card
- ☐ Rugged PC or Tablet
- ☐ Mobile Router (modem + Wi-Fi or multiradio technology)
- ☐ Vehicular Modem (single radio)
- ☐ None

Other (please specify)

Applications

What application(s) do you currently use on the existing wireless network? Check all that apply.

- ☐ Voice: Full Duplex
- ☐ Voice: Push-to-Talk
- ☐ Incident Reporting
- ☐ Database Lookups: Driver license, fingerprint retrieval, etc
- ☐ Email
- ☐ Web browsing
- ☐ Low Resolution Video (Web quality)
- ☐ High Resolution Video (TV quality)
- ☐ Mapping or Geospatial Data
- ☐ GIS-based Dispatch Data
- ☐ AVL or Telemetry Services (vehicles, personnel, offenders)
- ☐ Biometrics: Patient or Personnel
- ☐ SCADA for Facilities
- ☐ Software & Operating System Updates
- ☐ None

Other (please specify)

Subscribers Existing & Future

Please provide the following information regarding your estimated current and future wireless data devices. If you are unable to provide these quantities, please leave these questions blank and click "Next".

How many of each device does your agency currently operate on the existing wireless network?

_____ Smartphone or PDA
_____ Rugged Smartphone or PDA
_____ Embedded Cards (modem embedded inside computer
_____ Expansion Slot or USB Modem
_____ Rugged PC or Tablet
_____ Mobile Router (modem + WiFi or multiradio technology)
_____ Other

How many of each device would your agency plan to deploy by 2015 if a new statewide public safety broadband service was provided?

_____ Smartphone or PDA
_____ Rugged Smartphone or PDA
_____ Embedded Cards (modem embedded inside computer
_____ Expansion Slot or USB Modem
_____ Rugged PC or Tablet
_____ Mobile Router (modem + WiFi or multiradio technology)
_____ Other

Future Applications

How many users for each application would your agency plan to deploy by 2015 if a new statewide public safety broadband service were provided? If unknown, please skip.

_____ Voice: Full Duplex
_____ Voice: Push-to-Talk
_____ Incident Reporting
_____ Database Lookups: driver license, fingerprint retrieval, etc
_____ Email
_____ Web browsing
_____ Low Resolution Video (web quality)
_____ High Resolution Video (TV quality)
_____ Mapping or Geospatial Data
_____ GIS-based Dispatch Data
_____ AVL or Telemetry Services (vehicles, personnel, offenders)
_____ Biometrics: patient or personnel
_____ Software & OS Updates
_____ SCADA for Facilities

If not listed above, what other application(s) would you plan to deploy by 2015 on a wireless data network? Please also indicate the quantity of users that would use such applications.

Roaming

What percentage of your agency's users will regularly require roaming outside of the State of Minnesota. Please skip this question if you are unable to answer.

_____ Percentage of Roaming Subscribers

Coverage Requirement

Where do users in your agency need to use wireless data applications? Check all that apply.

- ☐ Outdoor
- ☐ Inside vehicle
- ☐ Inside single family home
- ☐ Inside large office buildings
- ☐ Inside brick or concrete buildings

Please describe your agency's anticipated wireless usage inside buildings and the applications and devices you intend to use indoors. Additionally, please indicate any other locations that require wireless coverage not indicated above.

Data Requirements for an Incident

Describe your wireless data needs at a major multi-agency incident. This could be either a past incident or possible future event. Possible examples can include “major flooding”, “bridge collapse”, “school shooting”, or “natural gas explosion”. Feel free to articulate an incident that best reflects your wireless data needs.

Please provide a brief description of the multi-agency event you will characterize in this section.

How many would respond?

_____ Personnel

_____ Vehicles

What applications are "mission critical" to your support at the incident?

- ☐ Voice: Full Duplex
- ☐ Voice: Push-to-Talk
- ☐ Incident Reporting
- ☐ Database Lookups: driver license, fingerprint retrieval, etc
- ☐ Email
- ☐ Web browsing
- ☐ Low Resolution Video (web quality)
- ☐ High Resolution Video (TV quality)
- ☐ Mapping or Geospatial Data
- ☐ GIS-based Dispatch Data
- ☐ AVL or Telemetry Services (vehicles, personnel, offenders)
- ☐ Biometrics: patient or personnel

Other (please specify)

Please provide any additional thoughts that you have regarding the goal(s), objectives, and requirements for a statewide public safety wireless data solution. What problems do you need a new broadband wireless service to solve? You can describe these goals in terms of coverage, reliability, type of service, etc.

Thank You

Thank you for taking the time to perform this survey. Your feedback will be carefully considered.

Kind regards,

The Wireless Broadband Requirements Project Team

13 APPENDIX E – NOTABLE WEB SURVEY FEEDBACK

- *Isanti Fire District: This is a FANTASTIC project. I have thought for years why this action is not in place. I see no issues with signal saturation utilizing the existing towers we already have in place.*

- *Le Sueur County Emergency Management: Currently we have limited wireless connectivity in our County EOC. A person has to go outside to make and receive cell phone calls.*

- *Polk County Sheriff: We have only air cards currently to cover our County that provide some of the above mentioned tasks/functions - our options are limited currently due to our geographical location. Long term goal would be to have full coverage at a reasonable cost.*

- *MDH - OEP: State should look to secure a contract with Satellite data service providers like Inmarsat, also Satellite phone service providers like Iridium. Currently have our units on the most basic or emergency plans to be cost effective.*

- *Lake County Emergency Management: Because our jurisdiction covers 2000 square miles, mostly remote and rugged terrain, we need MDC coverage broadband capability with real time voice and data capability and AVL. Due to our large wilderness areas and rescue requirements, portable and/or mobility.*

- *Waseca County Sheriff's Office: Coverage that is always there whether indoors or out.*

- *Lakeview Hospital: Needs to be robust-adequate speed and availability of a wide variety of end user devices. Coverage needs to be as good as the existing 800MHz voice system.*

- *Clay County Sheriff's Office: As part of the northwest Minnesota radio board I believe this would be a great opportunity for outstate Minnesota to utilize the towers on the state ARMER system. The problems I see if the cost is a lot more than utilizing private vendors.*

- *Metro Transit Police Dept: We would like the ability to conduct record checks with a hand held device when officer are on the trains, and buses and they don't have a squad car close to them*

- *Hovland Area Volunteer Fire Dept.: let's first solve a $6.2 billion state budget deficit.*

- *Hennepin EMS: My main issue right now is cost and the number of modems needed. I need 2 datacards per unit, for our MDC (mobile CAD) and our ePCR devices. I have been trying to get vehicle modems so we can go down to one connection and cut our costs in half.*

- *Nicollet County Sheriff's Office: Mainly a statewide system would give better coverage for our agency.*

- *Bemidji Fire Department: Need to effectively find locations and communicate with all personnel.*

- *Washington County Sheriff's Office: Sharing of information across disciplines, jurisdictions county and state lines.*

- *Dakota Communication Center: We need to be able to put the 9-1-1 network on a similar system to support continuity of operations with mutual aid capacity. We also need a radio system that this 99.99% reliable. As we grow, we need to be able to share with responders video, mapping, etc.*

- *Little Canada Fire Department: We need better coverage and cost.*

- *City of Duluth: We could highly benefit from a new broadband service - our main goals would be coverage and reliability and cost savings.*

- *Kandiyohi County: We need it to be fast and reliable - good coverage. Something that all agencies can utilize at a reasonable cost to said agencies. Provide the bandwidth for applications that we haven't yet considered using (face recognition software and auto license plate recognition).*

- *Polk Co Sheriff's Department: Not sure how to answer this question. Of course the best coverage and reliability would be ideal.*

- *Department of Public Safety: A Wireless Broadband data solution in MN must be reliable and coverage must be throughout the entire state with no loss of coverage even in remote areas. As they say, criminals know no boundaries!*

- *Roger's Two Way Radio: Seamless coverage indoors and outdoors everywhere, at least 100 mpbs speed, capacity for 200-300 personnel at a single site, encrypted, free access with no bandwidth limitation or maximum usage charges, no downtime, complete interoperability with commercial carriers.*

- *Homeland Security and Emergency Management: Must be reliable and be able to handle surges in service to provide the type of coverage you will need when an incident happens and it becomes a large hornets' nest at the site.*

- *Anoka County Central Communications: The primary requirement would be very high reliability, with at least minimally acceptable bandwidth for primary public safety functionality.*

- *Stevens Co Sheriff's Office: I believe the ability to share information, for officer and responder safety, as well as the timely recovery of the missing or vulnerable person would be aided by enhancing the reliability and robustness of the current wireless networks available.*

- *Saint Peter Police Department: A state resource would allow us to be less reliant on a commercial vendor and hopefully a more reliable system. If there are problems, we would have a more "local" contact to help resolve issues. I can't really complain about our current coverage.*

- *Nobles County Sheriff's Office: We just would like to have reliable service though out the county we have too many dead spots or spots with no service at all. Just help us get coverage.*

- *Stearns County Sheriff's Office: As with any technology application, the primary decision makers are cost and coverage. If the state could provide a reasonably priced option that provides seamless or near seamless coverage in and around our area, we would be interested.*

- *Cook County Sheriff's Office: The remoteness of Cook County currently does not allow for these types of applications. They are of limited value if only some of the agencies can connect to the services. It is important that the application and service be available to all agencies.*

- *Wayzata PD: Reliable coverage is important.*

- *Olmsted County Law Enforcement: A new systems major hurdles (in my opinion) are: Standardization, Cost, Maintenance, Support, Coverage Quality, On-going improvements, System / Interface capabilities.*

- *Mille Lacs Reservation DPS: GPS units cannot operate on Tribal Lands the Tribal Addresses will not be found or recognized there needs to be a way for Tribal Governments to be able to make the GIS system they use be able to accessed by emergency responders*

- *Goodhue County Sheriff's Office: We would be happy with a system providing service comparable with what we now have with Verizon. Our large fleet of air cards has the monthly rate down to about $20 per unit per month for unlimited air time. We would hope the proposed system would be cheaper.*

- *Minnesota Dept of Transportation: Communications are advancing so quickly for consumer uses that it would be difficult to build a state-owned system that would not be obsolete very quickly. Better to build on what the private sector is already doing for consumer uses.*

- *Ramsey County Emergency Communications: Cost effectiveness in providing state of the art throughput and services for a limited number of users (public safety) versus wireless carriers with large customer bases.*

- *MN State Fire Marshal Division: Reliable access throughout Minnesota is the primary issue for this office.*

- *Bureau of Criminal Apprehension: Much of what we provide is information to other law enforcement and criminal justice agencies. They then redistribute the data over their networks.*

- *Mahnomen County Sheriff's Dept: In an incident like whit which we had we had over a 100 different agency respond to this incident. Cellular Data coverage would have assisted us*

greatly; we mostly need better coverage and more reliability of the system working when needed.

- *Scott County: LTE systems do not currently have the range to be cost effective to deploy outside of the core metro area. Even in a suburban county, the number of sites needed to deploy LTE (in addition to existing 800MHz radio sites) would be cost prohibitive.*

- *Bemidji Ambulance Service, Inc.: The issue of having statewide, no dead or marginal areas of coverage is the main concern, or disappointment with virtually any wireless service subscriber. My take on this whole thing is that these companies are making hundreds of millions of dollars off*

- *Polk County So: Interactive between multiple agencies, such as fire, police and ambulance. Including dispatch*

- *Minneapolis Emergency Communications Center: Although the City's current Wi-Fi system is an excellent resource, it is not built out to neighboring communities, nor integrated with potential mutual aid scenarios. A common, possibly two or three tier system (metropolitan, community, rural) that could interconnect…*

- *Washington County S.O.: Would this be a system that would/could fail like cellphones on the day of the bridge collapse. In big events these systems often get overwhelmed. The ARMER system did not have any reported issues.*