Montana Public Safety Communications System Update

FirstNet: A Montana Prospective

Presented to the

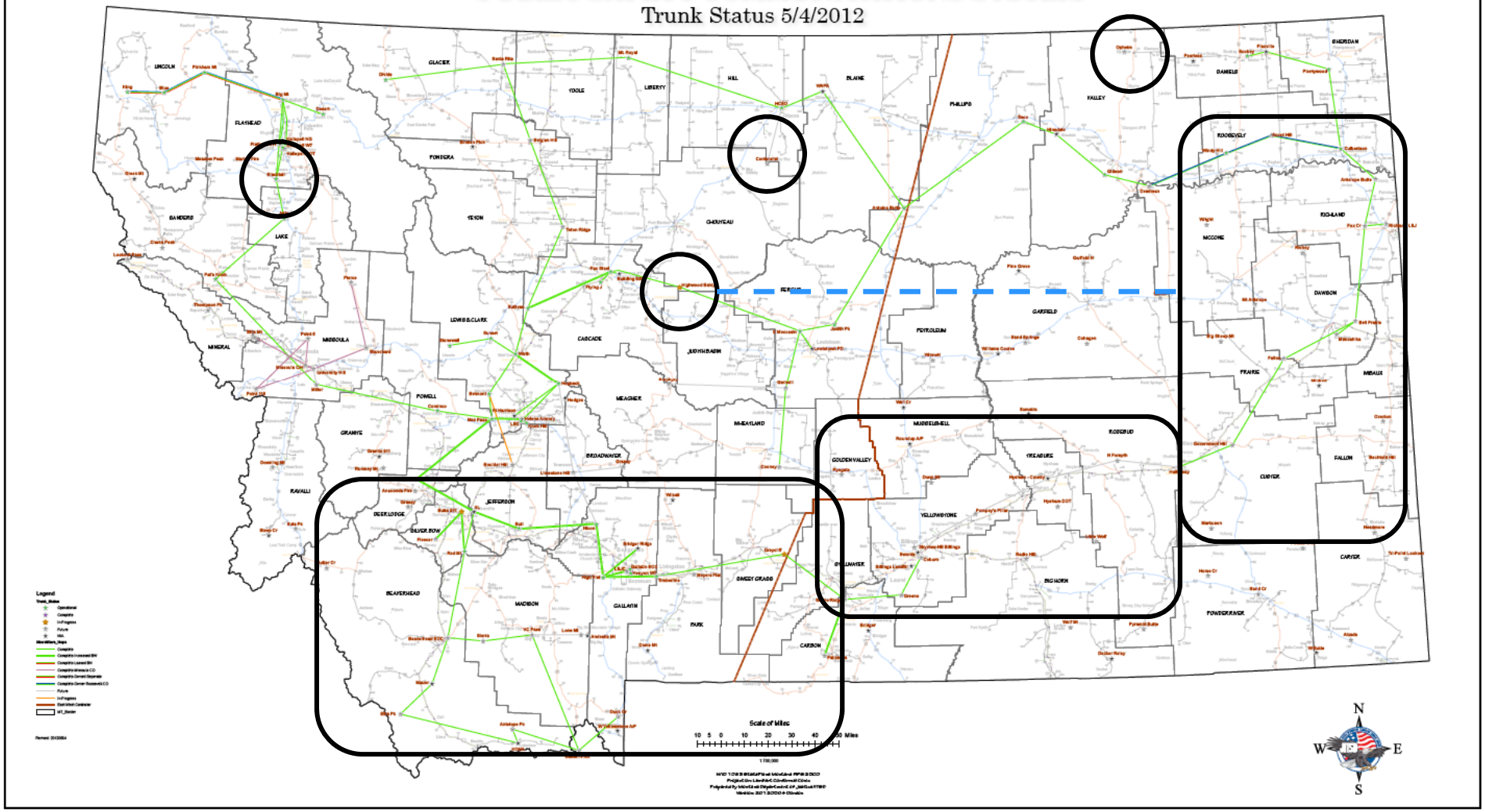
Energy and Telecommunications

Interim Committee

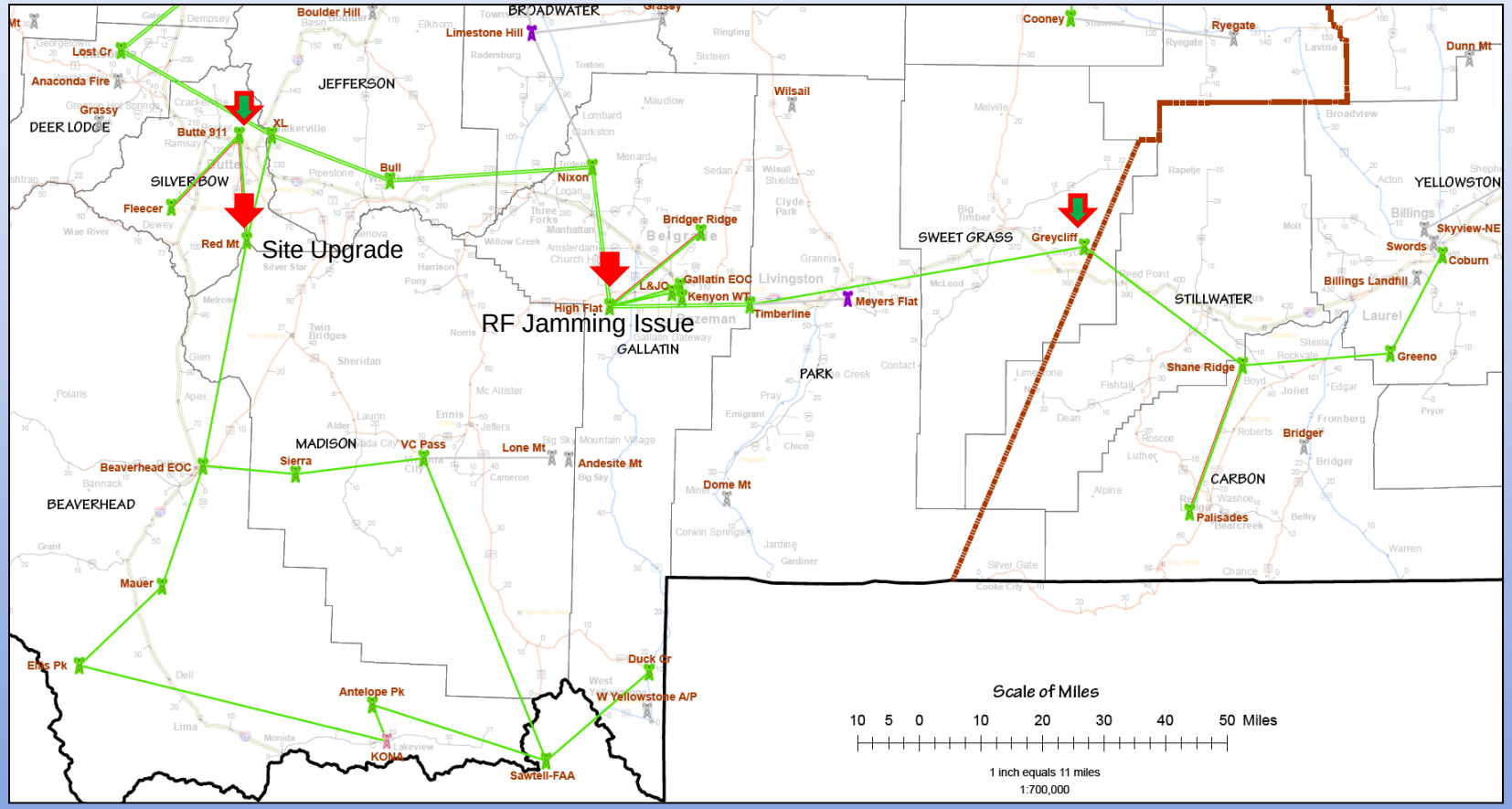
September 13, 2013

PUBLIC SAFETY COMMUNICATIONS SYSTEM

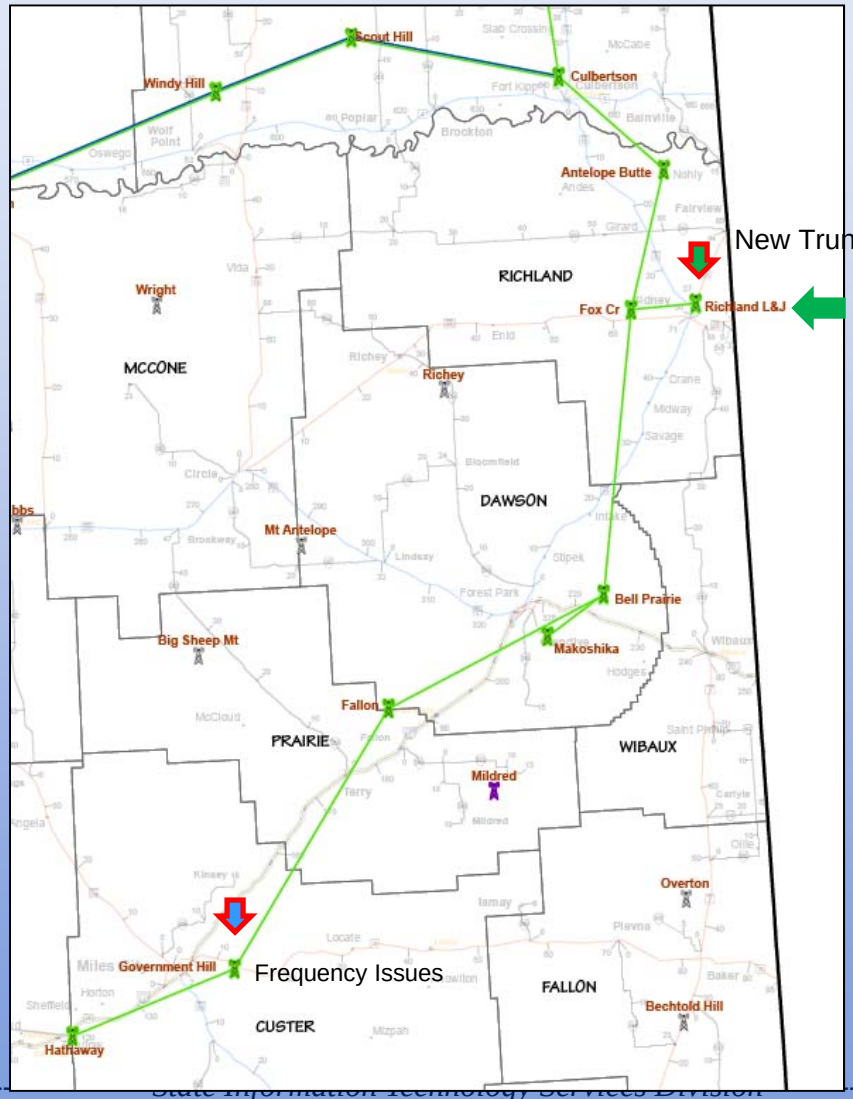
Trunk Status 5/4/2012



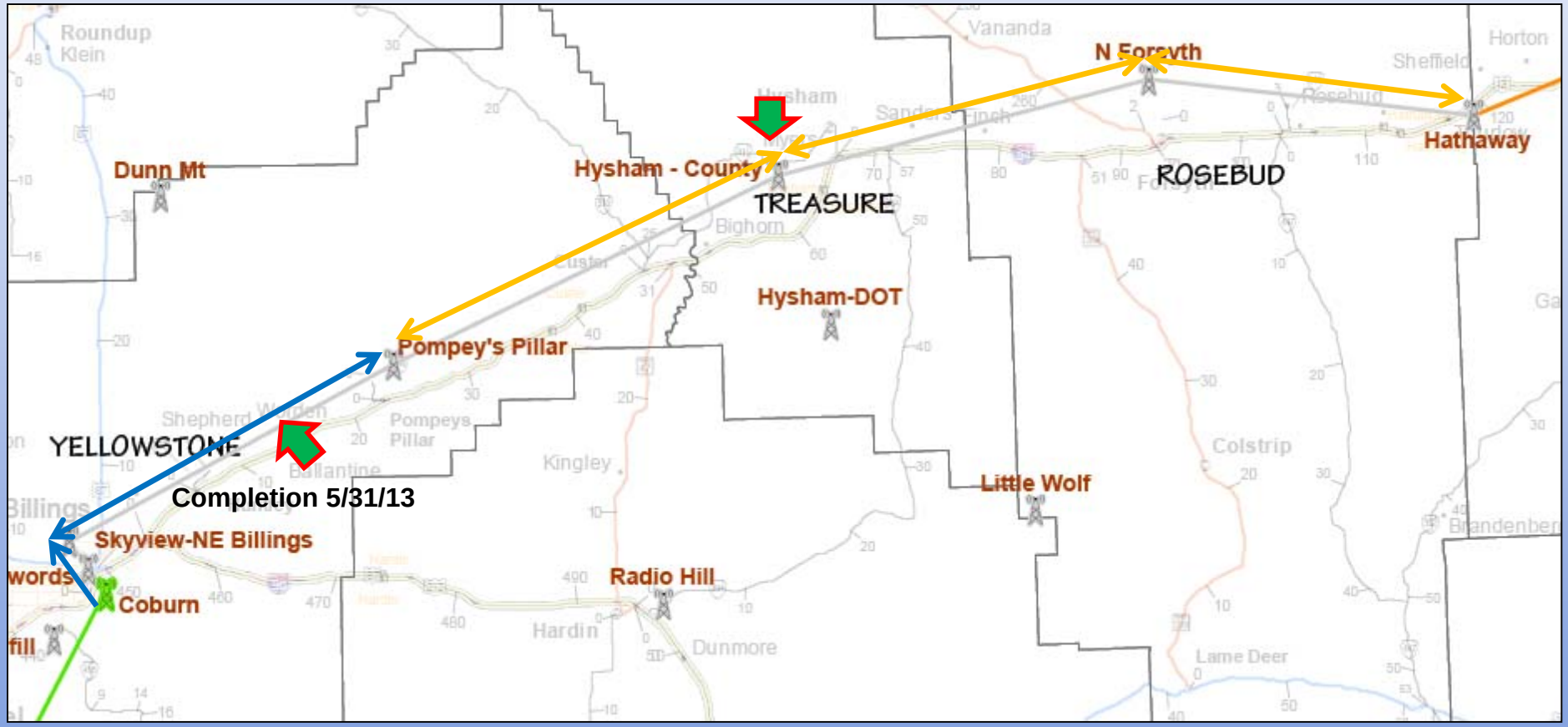
South West Trunking



North East Microwave & Trunking

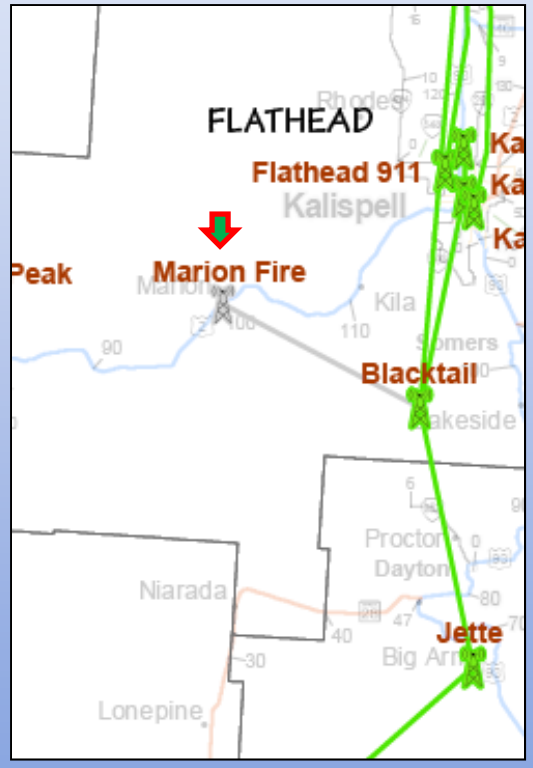


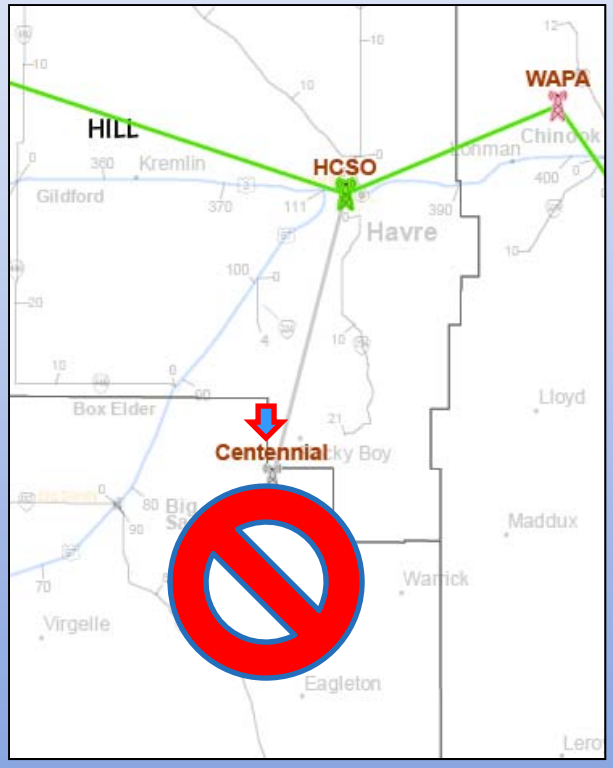
South Central Microwave

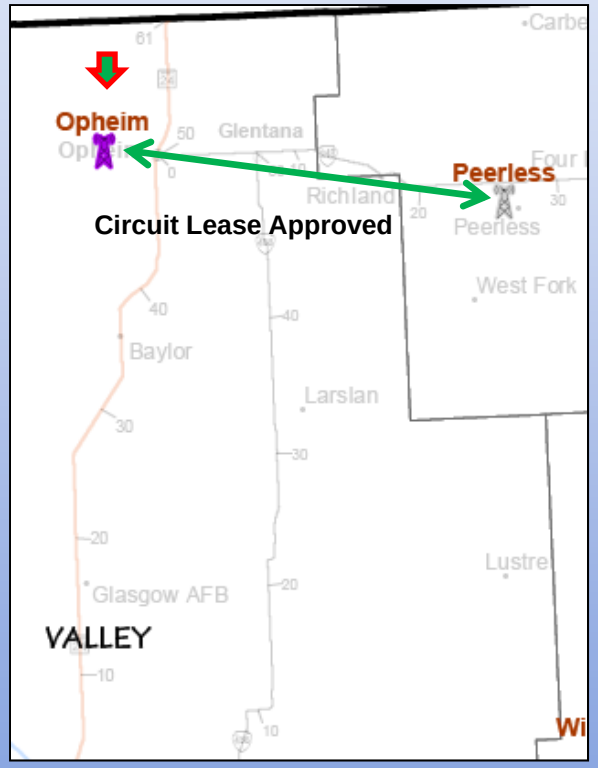


Hysham Site

Border Interoperability Demonstration Grant

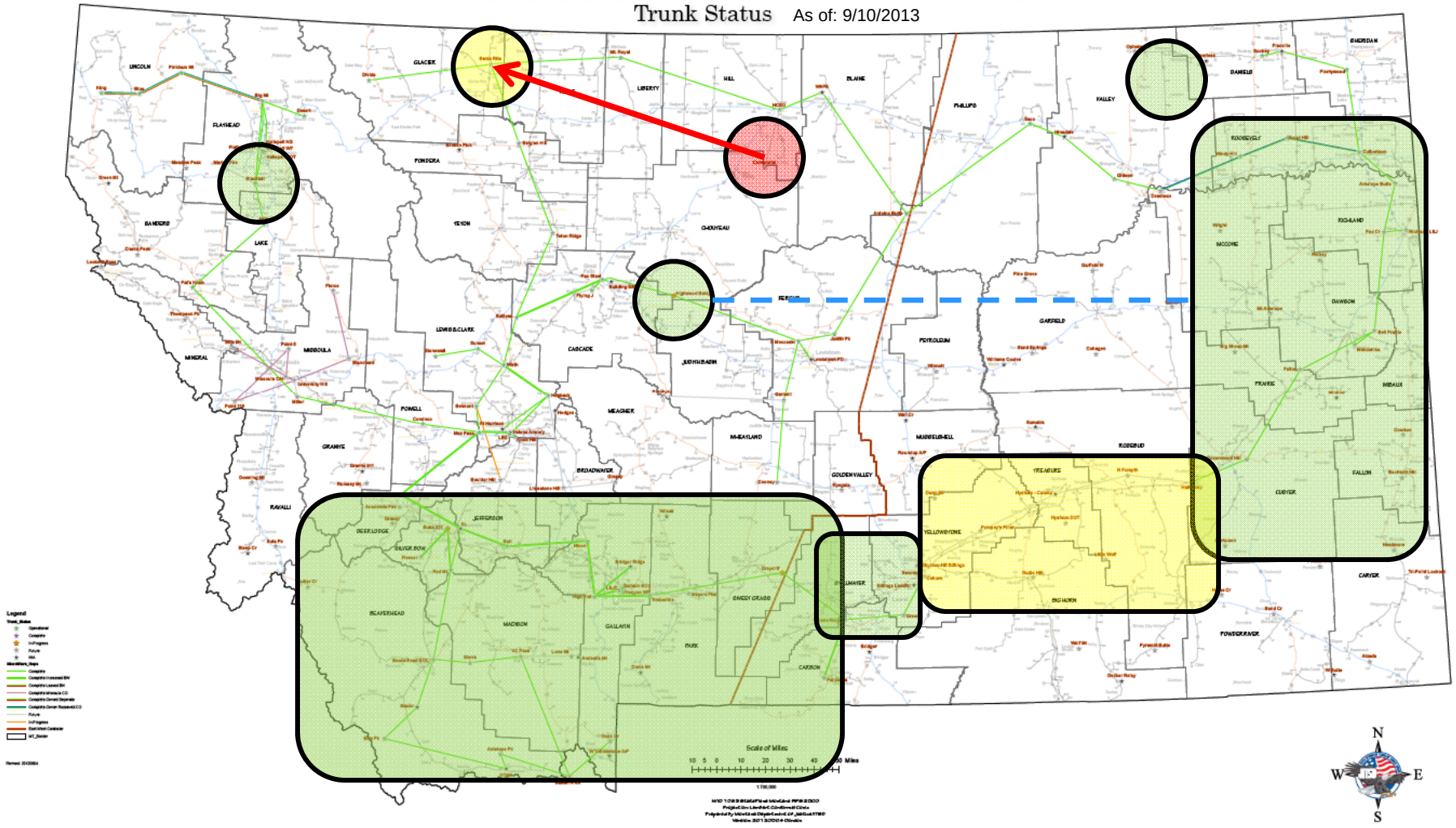






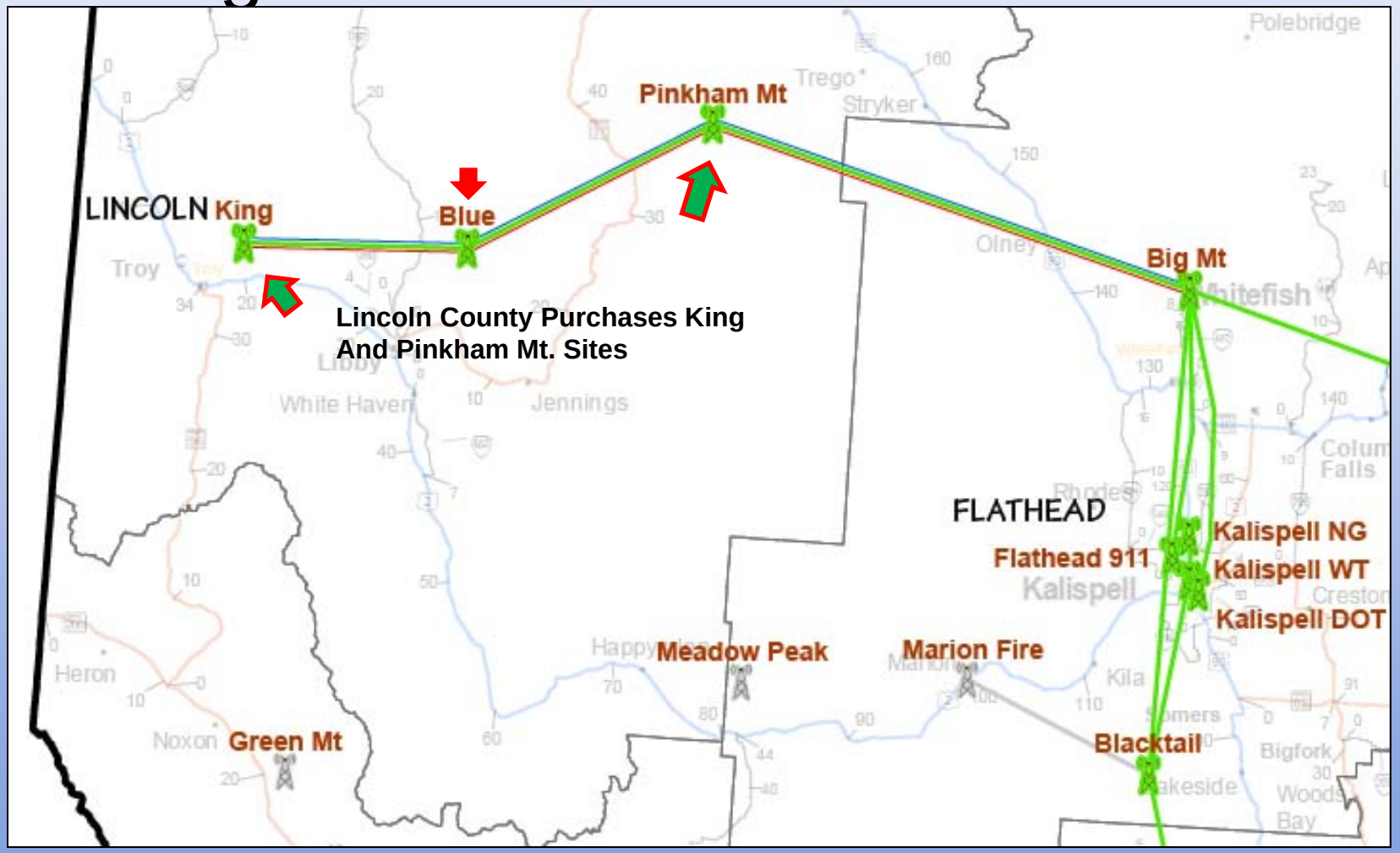
PUBLIC SAFETY COMMUNICATIONS SYSTEM

Trunk Status As of: 9/10/2013



63rd Legislature
Legislative Involvement
HB 10

Burlington Northern Lease



Public Safety Radio Systems – Current State

Land Mobile Radio (LMR) Systems

- Major Public Safety investment
- Mission Critical Voice
- 55,000 Public Safety Agencies
- Operating Across 6 Radio Bands
- Provides data capabilities

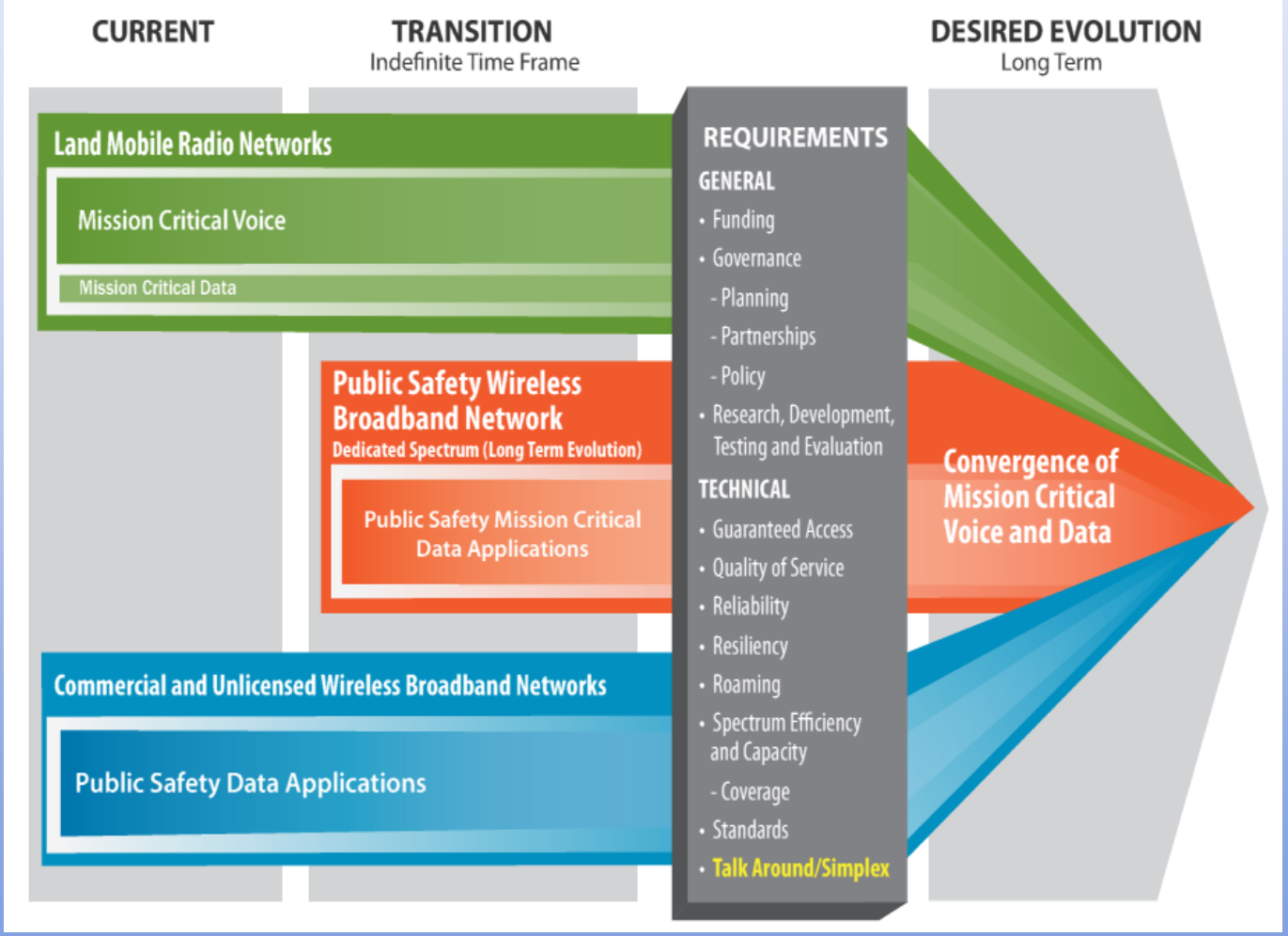
Public Safety Owned Data Systems

- Legacy technologies, some remain on analog wireless data systems
- Capacity, Speed, and Coverage less than current broadband offerings
- Use a mixture of technologies - RDLAP, Mesh, Point-to-point, point-to-multi-point, Muni-WiFi

Commercial Broadband

- Consumer grade of service
- No priority for Public Safety
  - Services may be inaccessible during significant events
- Available only where there is a significant customer base

Public Safety Communications Evolution



This conceptual framework outlines building wireless broadband data communications while maintaining LMR networks to support mission critical voice communications

Highlights of the Enacted Legislation

Middle Class Tax Relief and Job Creation Act of 2012

Title VI: Public Safety Communications and Electromagnetic Spectrum Auctions

Overview: Spectrum and Funding

On February 22, 2012, the President signed the Middle Class Tax Relief and Job Creation Act of 2012

- Spectrum Provisions
  - Reallocates the 700 MHz D Block spectrum to public safety
  - The Federal Communications Commission (FCC) is authorized to reallocate and auction the 470-512 MHz (T-Band) spectrum currently used by public safety entities within 9 years of enactment. Auction revenue will be used to reimburse relocation from the T-Band
- Funding Provisions
  - Authorizes the FCC to conduct incentive auctions to raise $7 billion for building and managing the Nationwide Public Safety Broadband Network (NPSBN)
  - Authorizes NTIA to provide $135 million to supports State and local efforts to plan and integrate with the NPSBN
  - Sets aside $20.4 billion in incentive auction revenue for deficit reduction

Technical Advisory Board for First Responder Interoperability

- Responsible for developing minimum technical requirements for the NPSBN to ensure nationwide interoperability
  - Requirements were based on Long Term Evolution (LTE) standards, and consultation with OEC, NTIA, and the National Institute of Standards and Technology (NIST)
  - The FCC announced members on March 22, 2012
- 14 voting members and 1 non-voting member:
  - Four represented public safety
  - Three represented state and local governments
  - Four represented wireless providers (two national, one regional, and one rural)
  - Three represented equipment manufacturers
- Submitted 46 recommendations and 55 major considerations in the following areas to the FCC on May 22, 2012, for FirstNet consideration for future network planning
  - 3GPP LTE Standards, Interfaces & Guidelines
  - User Equipment & Device Management
  - Testing
  - Evolution
  - Handover & Mobility
  - Grade of Service
  - Prioritization & Quality of Service
  - Security

Responsibilities of FirstNet

- ***Planning, constructing, operating, and managing the NPSBN***
- Building the network based on open, commercial standards for use and access
- Issuing and managing contracts with non-Federal entities to build and operate the network
- Establishing network policies
- Issuing requests for proposals for network build-out
- ***Encouraging the use of existing wireless infrastructure (commercial and/or public safety)***
- Act requires FirstNet to establish milestones for rural build-out & coverage
- ***Instructed to utilize "advantages offered through partnerships with existing commercial providers"***
- Consultation: On all matters below, FirstNet will consult with Federal, State, tribal, and local public safety entities, NIST, FCC and the public safety advisory committee
  - Management
  - Standards
  - Certified Equipment List
  - RFPs
  - Commercial Infrastructure
  - Cyber-Security
  - PSAPs
  - Rural Deployment
  - Prohibition on Consumer Service

State and Local Planning

- **Planning:** State, regional, tribal, and local jurisdictions will identify, plan, and implement the most efficient and effective way for such jurisdictions to utilize and integrate the infrastructure, equipment, and other architecture associated with the nationwide public safety broadband network

- **Funding:** State and local implementation Grant Program provides $135M to support planning and implementation efforts
  - NTIA, with FirstNet, must develop guidance within 6 months (August)
  - Requires 80/20% match unless waived by NTIA
  - ***Grant Program requires States to have designated a single officer or governmental body to serve as the coordinator of implementation of grant funds and interface with FirstNet***

On-Going Funding

FirstNet is expected to be self sustaining through the following funding mechanisms:

- **Network User Fee:** Fee from each entity including public safety or secondary user that uses the Network
- **Lease Fee for Network Capacity:** Fee for agreement between the FirstNet and secondary user to permit secondary access
- **Lease Fee for Network Equipment/Infrastructure:** Fee for entity that seeks access or use of antennas, towers, etc. constructed or owned by FirstNet

What is the Vision of FirstNet?

FirstNet Vision & Guiding Principles

FirstNet will provide communication tools that emergency responders need & deserve.

- Enable Unrestricted Communications
- Deliver Advanced Technology
- Leverage Scale to Lower Costs

FirstNet will provide dedicated spectrum, a single technology and funding to create a nationwide network dedicated to public safety.

Public Safety Effectiveness

- Dynamic Priority Access

Public Safety Grade

- Reliable
- Hardened
- Redundant
- Secure

Public Safety Applications

- 4G LTE for data and video
- Non mission-critical voice

FirstNet Will Augment LMR Systems

- **Public safety will rely on LMR for mission-critical voice for many years**
- **FirstNet can be co-located on existing LMR and commercial cellular infrastructure**
- **Sharing infrastructure will keep costs down and enhance coverage**

What is the FirstNet Business Model?

- Break Even and Build a Self-Sustaining Network
- User Fee for Network Service
- Leverage value of the spectrum
- Reflect value of contributed assets and partnerships

FirstNet Planning Process

What is needed: FirstNet requires input and requirements from state, local and tribal entities to prepare network plans for state review.

Examples include:

- Architecture of network
- Required coverage areas of the network
- Hardening, security, reliability, and resiliency requirements
- Assignment of priority users
- Network user training needs
- Availability of infrastructure that may be utilized

2013 Legislative Session

Public Safety Communications Legislation

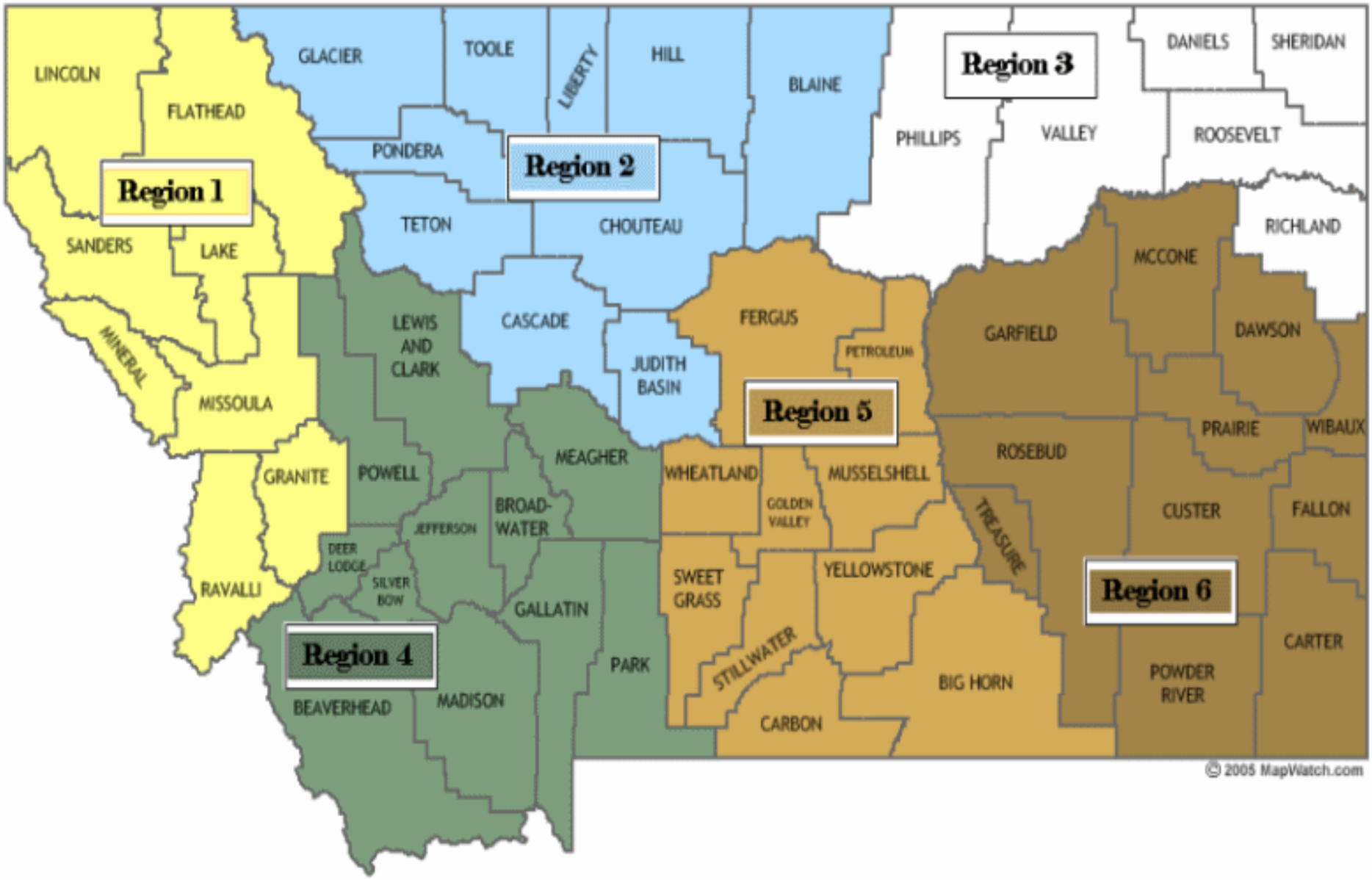
House Bill 2: $1,860,000 Federal Authority to expend U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA) Planning Grant awarded to the Montana Department of Administration.

First Responder Network Authority

http://www.ntia.doc.gov/category/firstnet

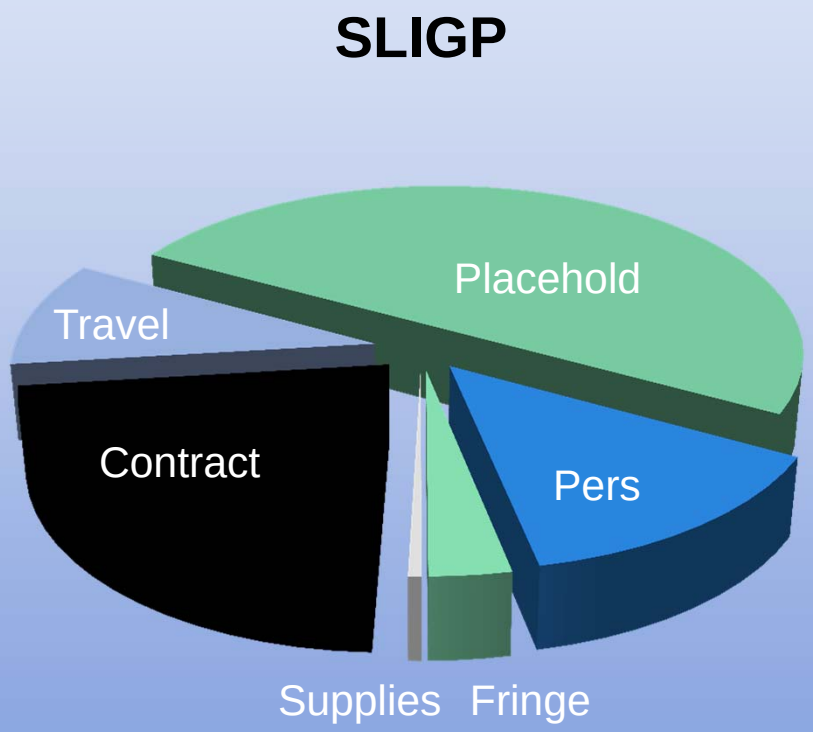
State and Local Implementation Program (SLIGP) Grant Activities:

- **Governance Board Requirements: OEC model with expanded representation**
- **Needs Assessment: Public Safety Disciplines by 64 Jurisdictions (56 counties, 7 tribes and state agencies) to inform the Consultation Process**
- **Education and Outreach to state, local and tribal governments and public safety disciplines to make them aware of FirstNet's broadband network deployment plans and service offerings**
- **Send local and state representatives to regional and national meetings (grant funds 8 regional and national meetings). "Pre-award meeting held at Denver, May 21- 22 Denver, Colo. Colorado. States represented: Kansas, Montana, Nebraska, New Mexico, North Dakota, South Dakota, Utah, Wyoming**
- **http://www.ntia.doc.gov/page/firstnet-state-consultation**
- **Answer Data Calls from FirstNet (yet to be determined); phase II federal funding ($908,208) will not be released until FirstNet completes its business plan**
- **RFP for contractors:**
- **Design needs assessment framework (may include questionnaires, on-line webinars, focus groups). What does the data tell us?**
- **Organize and schedule 3 meetings x 6 in-state regions = 18 meetings**


LINCOLN
FLATHEAD
GLACIER
TOOLE
LIBERTY
HILL
BLAINE
Region 3
DANIELS
SHERIDAN
PONDERA
Region 2
PHILLIPS
VALLEY
ROOSEVELT
Region 1
TETON
CHOUTEAU
SANDERS
LAKE
RICHLAND
MCCONE
LEWIS AND CLARK
CASCADE
FERGUS
GARFIELD
DAWSON
MINERAL
JUDITH BASIN
PETROLEUM
Region 5
MISSOULA
PRAIRIE
WIBAUX
ROSEBUD
MEAGHER
WHEATLAND
MUSSELSHELL
GRANITE
POWELL
BROAD-WATER
GOLDEN VALLEY
CUSTER
FALLON
JEFFERSON
TREASURE
DEER LODGE
SILVER BOW
SWEET GRASS
YELLOWSTONE
Region 6
RAVALLI
GALLATIN
CARTER
Region 4
PARK
STILLWATER
POWDER RIVER
BIG HORN
BEAVERHEAD
MADISON
CARBON
© 2005 MapWatch.com

Montana
State and Local Implementation Grant Program

SLIGP Preliminary Budget	Federal
Personnel	$250,000
Fringe	$ 56,850
Travel	$181,026
Supplies	$ 9,400
Contract	$410,931
Placeholder	$908,208
Total:	$1,816,415



SLIGP Governance

OEC Governance Model applied to NTIA
SLIGP Governance:
SWIC Becomes SWIC/SLIGP POC
SIGB expanded from 5 members to 13
SIGB oversees coordination of and makes recommendations to the Governor for LMR and Broadband Communications

Land Mobile Radio		**Broadband**
Office of Emergency Communications (OEC-DHS)	**From**	National Telecommunications and Information Administration (NTIA – DOC) **To:**
State of Montana Governor EO – 13-2011	**SIGB 5 members** →	**SIGB 13 members**
Statewide Interoperability Coordinator (SWIC) Warren Dupuis	**SIGB LMR Working Groups** →	**SIGB LMR *Broadband* Working Groups**
		Land Mobile Radio
		State of Montana Governor EO -
		SWIC –Quinn Ness SPOC –Warren Dupuis

FirstNet Issues RFIs on Technology for Nationwide Wireless Broadband Network

Potential Vendors and Partners Invited to Provide Information On Innovative Solutions for Core and Radio Access Networks

http://www.ntia.doc.gov/press-release/2013/firstnet-issues-rfis-technology-nationwide-wireless-broadband-network

FOR IMMEDIATE RELEASE:
July 10, 2013
News Media Contact:
(202) 482-0147, **press@firstnet.gov**

Questions from respondents are due July 22 and responses are due Aug. 30, 2013.

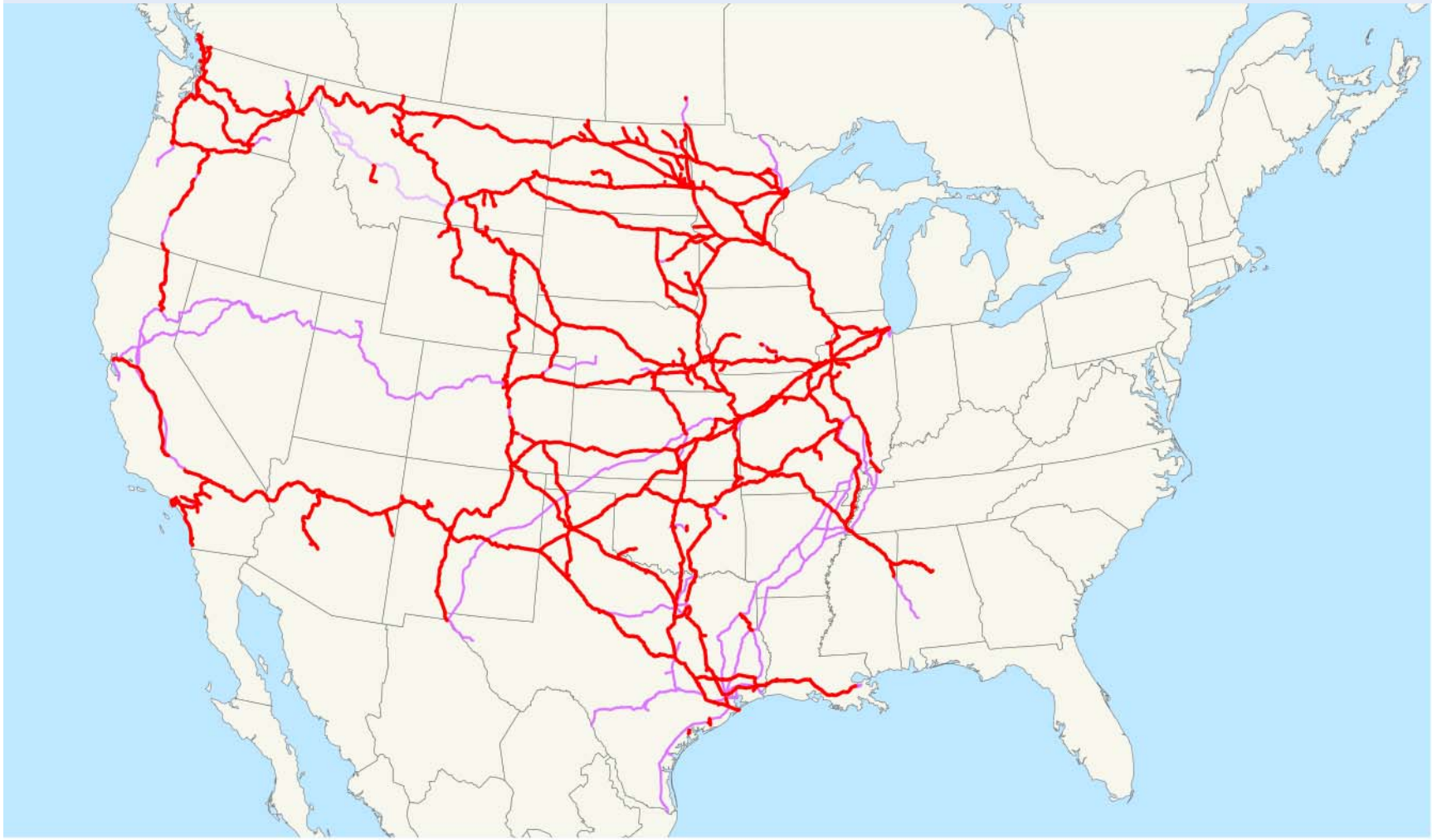
FirstNet Issues RFIs on Technology for Nationwide Wireless Broadband Network

Radio Access Network RFIs

1. Network Partnering and RAN Provisioning
2. Antenna Systems
3. Microwave Backhaul Equipment
4. Deployables
5. Satellite Service

Core Network RFIs

6. Enhanced Packet Core (EPC)
7. Transmission/Transport
8. Data Center
9. Network Management Center/Operations Management Center (NMC/OMC)
10. Network Service Platform



Questions?

SIGB New Executive Order

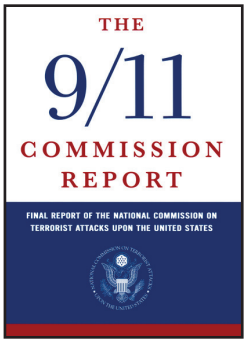
Using the “Whole Community Approach” the SIGB will likely be made up of representative from the same organizations participating on the 9-1-1 Advisory Council plus state public safety

- The Attorney General or his designee
- Governor’s Office representative
- The Montana State Chief Information Officer or his designee
- The Montana Department of Transportation Director or his designee
- The State Director of Indian Affairs
- A representative of the Montana Sheriffs and Peace Officers Association
- A representative of the Montana Fire Chiefs Association
- A representative from the Montana State Volunteer Firefighters Association
- A representative of the Montana EMS Association
- A representative of the Montana Association of Counties
- A representative of Montana Association of Chiefs of Police
- Two representatives of Montana Telecommunications Industry (non-voting)

Homeland Security
Office of Emergency Communications

December 2012

Nationwide Public Safety Broadband Network



Following the tragic events of September 11, 2001, the 9/11 Commission recommended the establishment of a nationwide, interoperable public safety communications network to resolve the communications challenges faced by emergency responders nationwide.

Since then, the public safety community has made progress in advancing emergency communications capabilities through enhanced coordination, governance structures, planning, training, and equipment. At the same time, private sector developments in high-speed, wireless communications technology have presented public safety with a platform to enhance information sharing and communications during emergencies and day-to-day operations. Through broadband technology, public safety users can have the ability to access video images of a crime in progress, download floor plans of a burning building, or connect rapidly and securely with personnel from other communities.

For the past decade, public safety has worked with State and local government officials, the Federal government, and Members of Congress to gather support for establishing a nationwide interoperable network. The U.S. Department of Homeland Security (DHS), through the Office of Emergency Communications (OEC) has helped set a broad policy framework for a nationwide interoperable networkto ensure it meets the needs of its users and aligns with existing emergency communications policy.

On February 22, 2012, President Obama signed into law H.R.3630, the Middle Class Tax Relief and Job Creation Act of 2012, which includes provisions to fund and govern a Nationwide Public Safety Broadband Network. OEC is working with the Departments of Commerce and Justice to ensure it meets the needs of users in the public safety community.

BENEFITS OF THE NATIONWIDE PUBLIC SAFETY BROADBAND NETWORK

The Nationwide Public Safety Broadband Network will provide a secure, reliable and dedicated interoperable network for emergency responders to communicate during an emergency.

Supporters secured the "D Block" – a 10 Megahertz (MHz) section of radio spectrum adjacent to 10MHz currently licensed to public safety – to be used for the nationwide network. This will provide 20 MHz of spectrum solely dedicated for the use of emergency responders and ensure they have adequate network capacity, which often becomes congested during an emergency situation.

NATIONWIDE GOVERNANCE: FIRSTNET

A key provision of the law created the First Responders Network Authority (FirstNet), an independent authority within the Department of Commerce's National Telecommunications and Information Administration (NTIA). FirstNet is responsible for deploying the Nationwide Public Safety Broadband Network.

The Act licenses the existing public safety broadband spectrum and the 700MHz D Block spectrum to

FirstNet. FirstNet is responsible for, at a minimum, ensuring nationwide standards for use and access of the network; and issuing open, transparent, and competitive requests for proposals (RFPs) to build, operate, and maintain the network. It is also responsible for leveraging, to the maximum extent economically desirable, existing commercial wireless infrastructure to speed deployment of the network; and overseeing contracts with non-federal entities to build, operate, and maintain the network.

There are 15 members of the FirstNet Board of Directors. Three of those are permanent Federal members: the Secretary of Homeland Security, the US Attorney General, and the Director of the Office of Management and Budget. The Secretary of Commerce appointed the other 12 members of the FirstNet Board. These remaining members represent the interests of State, local, territorial, and tribal government; public safety; finance; and technology.

A standing public safety advisory committee, established by the Act, will assist FirstNet in carrying out its duties. In addition, to ensure the input of State and local stakeholders is recognized, the Act also requires FirstNet to consult with State and local entities throughout network deployment.

FUNDING

The Act also establishes the Public Safety Trust Fund to direct funding from voluntary incentive spectrum auctions for the following priorities:

- **State and Local Implementation Grant Fund** The Act establishes a grant program to assist State, local, and tribal jurisdictions with identifying, planning, and implementing the most efficient and effective means to use and integrate the infrastructure, equipment, and other architecture associated with the Nationwide Public Safety Broadband Network. Up to $135 million was made available to NTIA for the State and Local Implementation Grant Program.
- **Network Construction Fund** The Fund provides $7 billion for FirstNet to deploy and operate the NPSBN, not including administrative costs.
- **Research Funding** The Fund provides $100 million to NIST in consultation with the FCC, DHS, and DOJ, to research and develop standards, technologies, and applications to advance wireless emergency communications.
- **NG9-1-1** The Fund provides $115 million to support deployment and operation of 9-1-1 services. These funds are only available after $20.4 billion is raised for deficit reduction.
- **Additional Research Funding** After all previous funding priorities, an additional $200 million is allocated to NIST for further research efforts.

SUPPORT FOR STATE, LOCAL, AND TRIBAL IMPLEMENTATION

Since OEC was established by Congress, a key component to our efforts has been, and will continue to be, engagement and collaboration with public safety and government at the Federal, State, local, and tribal levels. As this new network is developed and deployed, this engagement will be more important than ever.

OEC is offering on-site support through its Technical Assistance (TA) Program to assist users with an understanding of broadband technology and early planning for its use in public safety operations. The TA Program is also supporting States in incorporating broadband planning into their Statewide Plans through workshops being held across the country. State and local agencies can begin preparing for wireless broadband implementation by analyzing their existing Statewide Plans and Governance Bodies and determining if changes need to be made.

FOR ADDITIONAL INFORMATION

Please contact OEC@dhs.gov or visit www.dhs.gov (keyword OEC).

October 2012

The Nationwide Public Safety Broadband Network
FAQs for Policymakers

The *Middle Class Tax Relief and Job Creation Act of 2012* (the Act), specifically Title VI entitled *Public Safety Communications and Electromagnetic Spectrum Auctions*, authorizes the deployment of the Nationwide Public Safety Broadband Network (NPSBN). The NPSBN will be a wireless, interoperable nationwide communications network that will allow the public safety community to securely and reliably gain and share information with their counterparts in other locations and agencies. The law also establishes the First Responder Network Authority (FirstNet) as an independent body that will govern the NPSBN; sets aside $7 billion for network development, deployment, and operation; and assigns the use of the 700 MHz D Block to FirstNet for the public safety community. As envisioned, the network will incorporate open, commercial wireless technology standards.

NATIONWIDE NETWORK OVERVIEW

What is the purpose of the NPSBN? As envisioned, the network will allow first responders to send and receive voice, video, and other information in real time; enable communications across agencies and jurisdictions; and improve the safety and effectiveness of operations by enhancing the way public safety personnel are notified about, gain information on, and respond to emergencies and natural disasters.

What is the history of the NPSBN? Following the terrorist attacks on September 11, 2001, the 9/11 Commission was established to review the incident and make recommendations to the President that would mitigate the possibility of such attacks occurring again. One of the 9/11 Commission's recommendations was the establishment of a nationwide, interoperable public safety communications network envisioned to resolve communications challenges faced by emergency responders. For the past decade, public safety worked with State and local government officials, the Federal government, and Members of Congress to amass support for the creation of the nationwide network. On February 22, 2012, President Obama signed the Act into law, of which Title VI includes provisions to fund and govern the NPSBN.

What is FirstNet and what will it do? FirstNet is an independent authority within the Department of Commerce's National Telecommunications and Information Administration (NTIA) that will develop and design the network architecture and gather network requirements. FirstNet will also develop a plan for network deployment for each State; and work with State, local, and tribal governments to create an interoperable, nationwide network; and hold the spectrum license for the NPSBN. FirstNet is led by a Board composed of 15 members including the Secretary of Homeland Security, the Attorney General, the Director of the Office of Management and Budget, and 12 experts—named by the Secretary of Commerce on August 20, 2012—each with experience in the public safety, technical, network, or financial fields. Per the Act, at least three Board members must represent the collective interests of States, local, tribes and territories. Additionally, at least three Board members must have served as public safety professionals.

When will the NPSBN be deployed? There is no defined timeline for the deployment of and transition to the NPSBN. FirstNet must first engage in a consultation process before crafting its nationwide network architecture, which will serve as the basis for

requests for proposal (RFPs). FirstNet will provide each State with a proposed network build-out plan and State-specific funding allocation, as determined by NTIA.

Will deployments vary across the country? It is projected that deployments will vary by State based on existing infrastructure and geography; however, the way in which deployments will vary will not be known until FirstNet develops the plan for each State.

What entities are included in the term "public safety"? The Act defines a public safety entity as a provider of public safety services and defines public safety services and emergency response providers by the definitions included in the Communications Act of 1934 and the Homeland Security Act of 2002, respectively. Section 337(f) of the Communications Act defines public safety services as the sole or principal purpose of which is to "protect the safety of life, health, or property; that are provided by State or local government entities; or by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and that are not made commercially available to the public by the provider." Section 2 of the Homeland Security Act of 2002 defines emergency response providers as including "Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities."

What is the timeline for my State to opt-out of the NPSBN? Within 90 days of a State receiving the FirstNet plan for the NPSBN, the governor of each State must decide whether to participate in the FirstNet recommended nationwide network build-out or opt-out and deploy a State-specific Radio Access Network (RAN) that connects to the nationwide network. If the governor elects to opt-out, the governor must develop and complete requests for proposals for the construction, maintenance, and operation of the RAN within 180 days of notifying FirstNet, NTIA, and the Federal Communications Commission (FCC) of its decision. The State must submit to the FCC an alternative plan for RAN construction and operation that meets the minimum technical interoperability requirements developed by the Technical Advisory Board for First Responder Interoperability and interoperates with the NPSBN. The State must also apply for spectrum through the NTIA and pay user fees for the shared elements of the network core. The State may also apply to NTIA for a grant to build, its portion of the RAN. If the FCC disapproves the State's plan, network build-out within the State will proceed under the FirstNet plan.

A commercial vendor has offered to sell Long Term Evolution (LTE) infrastructure to my agency. Do I need to purchase this equipment now? No, you do not need to purchase, and in some cases should not purchase, LTE infrastructure and devices from commercial vendors at this time. Because the network architecture has not been designed or deployed, it is impossible to know what infrastructure and devices each State, region, or jurisdiction may need. Any entity making such purchases now risks buying infrastructure and equipment that may not be interoperable with the future NPSBN.

COMMUNICATIONS TECHNOLOGY

What is the difference between Land Mobile Radio (LMR) and broadband networks, in particular LTE networks? LMR is a terrestrially-based wireless narrowband communications system commonly used by Federal, State, and local emergency responders, public works companies, and even the military to support voice and low-speed data communications. LTE is the next evolution of commercial broadband wireless communications technology, which was developed to address the demand for high-speed, data intensive communications, such as situational awareness, advanced analytics, database lookups, and video applications. LTE promises higher data transmission rates and capacity than the current 3rd generation (3G) commercial service offerings. Unlike LMR, LTE does not currently support mission critical public safety grade voice communications; priority access for public safety users; or have the push-to-talk, multi-broadcast, or the ability to talk device-to-device (known as "talk around") capabilities required by the public safety community. Additionally, FirstNet's deployment is likely to be a multi-year rollout, so coverage may not be ubiquitous from the outset.

What is the difference between public safety and commercial networks? Public safety voice and data networks are designed to provide emergency responders with dedicated communications networks. Public safety

networks require higher degrees of robustness, resiliency, redundancy, and security than commonly found in commercial networks. Public safety networks are built to provide equal coverage across broad areas, handle one-to-many communications, and data distribution wherever the incident or event occurs. Commercial communications networks provide primarily one-to-one communications services to private consumers and are designed to generate the largest possible economic return for the commercial provider.

While current commercial solutions are used to augment public safety networks by providing non-mission critical services, many commercial mobile data solutions are not interoperable with public safety data systems. In addition, commercial mobile data have limited bandwidth and capacity, are not built to public safety standards, do not provide priority for first responders in the event of an emergency, and may become inaccessible during a significant emergency event.

Will broadband replace LMR? For the foreseeable future, broadband will supplement, but not replace LMR. At this time, the available broadband technologies do not adequately support voice communications capabilities as required by public safety personnel; therefore, it will be necessary to continue to invest in LMR networks as an integral part of first responder communications. Voice over LTE (VoLTE) standards are under development and emerging, and in time may provide standardized voice capabilities as an adjunct to public safety LMR services. These VoLTE services will be similar to telephony services and capabilities now offered on commercial 3G systems. While VoLTE is expected to support standardized voice traffic over LTE, the way in which critical LMR voice capabilities can be delivered in the NPSBN in the future will only be determined once the architecture is defined; technical standards are drafted and accepted; devices are built, tested, and certified; and the public safety community begins the migration to these new services and capabilities.

GOVERNANCE

Who is responsible for coordinating all the State and local assets and working with the FirstNet Board? The Act requires each State to designate a single State officer or governmental body that will be the point of contact for consultations with FirstNet. States must also designate a single officer or governmental body to coordinate the implementation of any grant funding the State receives under the State and Local Implementation Grant Program. These decisions will be made by each State's governor. Many States have a Statewide Interoperability Coordinator and a Statewide Interoperability Governing Body to implement the statewide plans for enhancing interoperable communications. These individuals and structures should be leveraged to support NPSBN implementation.

FUNDING

How will the network be funded? The Act authorizes the creation of the Public Safety Trust Fund (PSTF), in which revenue collected from the spectrum auctions will be deposited, to fund FirstNet's activities as it designs, deploys, operates, and maintains the network. FirstNet also will collect user fees and fees from leasing its spectrum, and is also authorized to accept other financing, such as through grants and gifts.

Will funding of the network raise taxes in my State? Per the legislation, funding for the network will be generated by spectrum auctions through Fiscal Year 2022, not through tax revenue. Sustainment of the network is envisioned to come from user fees and potential leases of network assets to private sector providers for secondary use.

Is grant funding available to develop a network in my State? Will this funding pay for planning only, or also for equipment or services? While grant programs and funding have been identified, currently there is no structure to apply for and receive funding. In the future, NTIA will provide guidance regarding how to apply for funds from the State and Local Implementation Grant Program, define the scope of eligible grant activities, and prioritize grants for activities that ensure both rural and urban network coverage.

Does the size of my State matter or will most of the funding go to States with larger populations? If the State has many tribal entities, does that impact how much money a State may get? Distribution of grant funding for State and local planning for broadband has not yet been determined. The Act contains no provisions that indicate certain areas will receive more funding than other regions of the country. At this time it is also undetermined how the prevalence of tribal entities in a State will impact funding.

How much will the network cost to develop, deploy, and maintain? For what percentage of this cost will States and local areas be responsible? At this time, it is unknown how much it will cost to develop, deploy, and maintain the NPSBN; thus, there is no specific information available to indicate what percentages may be attributable to State or local entities. Any qualified entity receiving support through the State and Local Implementation Grant Program and State construction grant funding will be required to provide a minimum of a 20 percent match, unless a waiver is obtained.

Should I continue to spend money on public safety communications systems? Public safety's use of LMR systems will continue for the foreseeable future as there is no defined timeframe when LTE broadband technology may provide the same level of mission-critical voice services that are available today. Therefore, it will be necessary to continue investments for existing and new LMR voice systems, while allocating new funding to the development and deployment of the NPSBN.

Can my State generate revenue from the NPSBN if we opt-out? No. If a State chooses to opt-out it is only opting-out of the provision and construction of the RAN portion of the envisioned network. The Act specifies that if a State chooses to opt-out and then satisfies all of the conditions to construct a State-provided RAN using grant funding from FirstNet, any money or fees collected must be used to support the constructed network.

IMPACT AND THE FUTURE OF THE NETWORK

What do I need to do to promote the development and deployment of the NPSBN? The network build-out will require continuing education and a high level of commitment at all levels of government and across public safety disciplines to understand network requirements and identify existing resources and assets. It will also be necessary to develop and maintain strategic partnerships with a variety of stakeholder agencies and organizations, and design effective policy and governance structures. Stakeholders must engage in planning and coordination at the nationwide, statewide, regional, and tactical levels; foster partnerships between disciplines and jurisdictions; and develop policies and plans for new and emerging emergency communications technologies.

Has such a deployment been done successfully elsewhere? While there are regions that have received grant funding and invested their own resources to develop a network using broadband technology, no such nationwide public safety network exists in the US today. Further, while no other nation has developed a broadband network for public safety, nation states throughout the world, primarily in Europe and Asia, have built TETRA and TETRAPOL voice and data systems for emergency responders. In North America, the National Law Enforcement Telecommunications System (NLETS) network provides law enforcement and public safety personnel in the US and Canada with the ability to exchange information and other data. Other Federal networks, such as the Federal Bureau of Investigation's National Crime Information Center, Automated Fingerprint Identification System, and State Criminal Justice Information Systems, are accessible by authorized law enforcement entities at all levels of government.

FOR ADDITIONAL INFORMATION

Please contact **OEC@dhs.gov** or visit **www.dhs.gov** (keyword OEC).

Homeland Security
Office of Emergency Communications

October 2012

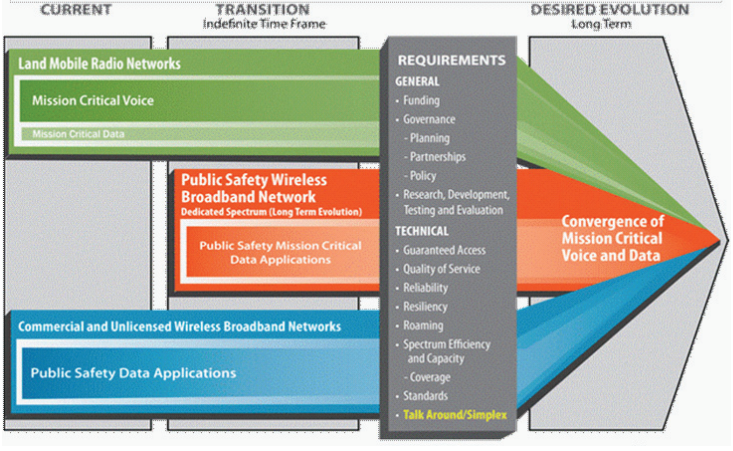
Realizing the Future of Public Safety Communications

The evolution of wireless data communications **driven by commercial providers** has led to on-demand access to information, data, and applications for consumers worldwide; however, the expansion of available data services **has largely bypassed emergency responders.** Although first responders across the United States currently use Land Mobile Radio (LMR) networks and commercial/agency-specific wireless technology, the passage of the Middle Class Tax Relief and Job Creation Act of 2012 (the Act) should position the community to fully leverage advancements in Long Term Evolution (LTE) technology in developing and deploying an interoperable, Nationwide Public Safety Broadband Network (NPSBN). While incompatible and outdated communications equipment, as well as **overloaded commercial networks, has** hindered public safety, the NPSBN will eventually provide the emergency response community with mission critical voice, data, and video capabilities and access to real-time information. As a result, first responders will be able to communicate across agency and jurisdictional boundaries, enhance the effectiveness of emergency communications nationwide, and assist responders in conducting safer and more effective operations.

TODAY'S PUBLIC SAFETY COMMUNICATIONS ENVIRONMENT

Presently, the public safety community receives mission critical voice services through its dedicated LMR networks. While currently available commercial wireless and broadband data solutions are adequate for non-mission critical or auxiliary use, the majority of these solutions have limited ability to fully support emergency responders because they are not interoperable, have limited or constrained bandwidth availability, are subject to loss during periods of heavy use, and are not built to public safety standards. However, the Act creates a pathway to overcome these challenges by reallocating the 700 MHz D Block spectrum to the public safety community and sets aside up to $7 billion for the development and deployment of the NPSBN. Until FirstNet – an independent authority, within the Department of Commerce National Telecommunications and Information Administration, authorized by the law to take all actions necessary to ensure the design, construction, and operation of the NPSBN – is established and operational, much of the timeline for network deployment and planning activities each State and locality is yet to be defined. Additionally, the Act provides $135 million for State and local implementation planning grants, however the government has not yet made these dollars available or established a structure to apply for and/or receive the necessary funding.

Figure 1. The evolution of public safety communications toward a convergence of mission critical voice and data.



PUBLIC SAFETY COMMUNICATIONS OF THE FUTURE

This NPSBN, combined with existing LMR, holds the promise to drastically advance public safety's ability to communicate information during emergencies. In order to achieve this vision, the public safety community, policymakers, and other stakeholders must continuously address key requirements (see Figure 1) including funding, governance, R&D, and other technical aspects. Portions of the law will help to address some of these requirements, such as sections pertaining to access, roaming, and implementation funds. The pace of convergence will vary from agency to agency and will be influenced by various factors such as operational requirements, existing systems, deployment schedules, and funding levels. While currently there is no defined point in time when broadband will support mission critical voice, once the convergence of voice and data has occurred emergency responders will have access to advanced technologies and applications that should improve their operational capabilities, response efforts, and delivery of services.

REALIZING THE FUTURE

Developing an interoperable NPSBN and realizing effective convergence with existing capabilities will require a high level of commitment from stakeholders at all levels to identify adequate and sustainable funding sources, develop and maintain partnerships, and design effective policy and governance structures. Because there is no definitive timeframe when the NPSBN will be deployed and functional for first responders, it will be necessary to continue to invest in existing infrastructure, LMR voice systems, and maintain current commercial and unlicensed wireless and broadband data solutions, while simultaneously allocating new funding to the development and deployment of the NPSBN. Additionally, stakeholders must engage in planning and coordination at the nationwide, regional, State, and local levels; foster partnerships between disciplines and jurisdictions; and develop policies and plans for new emergency communications technologies. These commitments to stable funding, appropriate partnerships, and effective policy and governance structures will enable the public safety community to take advantage of new advances in technology and realize the promise of an interoperable, nationwide public safety communications network.capabilities, response efforts, and delivery of services.

Keys to Effective Network Convergence:

√ Maintain adequate funding for LMR and the NPSBN

√ Develop appropriate partnerships at all levels

√ Design effective policy and governance structures

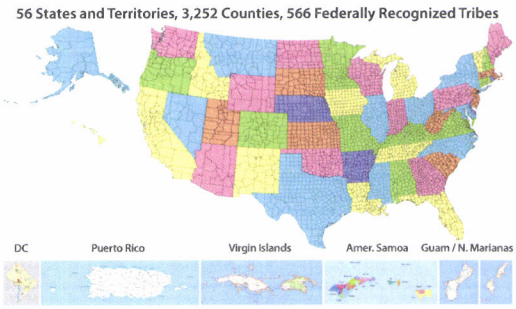
FOR ADDITIONAL INFORMATION

Please contact **OEC@dhs.gov** or visit **www.dhs.gov** (keyword OEC).

The Promise of FirstNet

What is FirstNet?

FirstNet will be the first high-speed wireless, broadband data network dedicated to public safety. FirstNet will be a single, nationwide network that facilitates communication for public safety users during emergencies and on the job every day. Think of FirstNet as a bigger, more reliable, secure and resilient "wireless pipe." This new network will be public safety-grade, providing access to applications and coverage where public safety needs it most.



What will be possible with FirstNet?

Initially FirstNet will be used to send data, video, images and text and make cellular-quality voice calls. Users will get fast access to information they need to meet their mission. Unlike commercial wireless networks, FirstNet will allow for priority access among public safety users. FirstNet will also give incident commanders and local officials control over the network so, for example, they can assign users and talk groups and determine who can access applications.

Why was FirstNet created?

After 9/11, the public safety community fought hard to fulfill the 9/11 Commission's last standing recommendation and convince Congress that it needed a dedicated, reliable network to provide advanced data communications capabilities nationwide. Commercial networks get overloaded or fail and don't provide priority access to public safety users during emergencies.

How will FirstNet benefit public safety?

Using FirstNet will improve situational awareness and decision-making. Just as smartphones have changed our personal lives, FirstNet devices and applications will ultimately change the way public safety operates. FirstNet will save time during emergencies when seconds count. FirstNet will save money for states by leveraging nationwide purchasing power and scale economies. Using FirstNet can help save lives, solve crimes and keep our communities and emergency responders safer.

How will states and agencies participate in the buildout of FirstNet?

To make FirstNet a nationwide network, all states must have a local radio access network (RAN) that connects to the FirstNet core. FirstNet is responsible for working through the designated state point of contact to consult with states, local communities, tribal governments and first responders to gather requirements for developing its RAN deployment plan. If the FirstNet plan is accepted by a state, FirstNet will construct the RAN. If a state prefers to build its own RAN, the state must secure FCC approval and may seek funding support from NTIA. State-built RANs must meet FirstNet security, hardening and interoperability requirements.

What will users pay for FirstNet services?

FirstNet intends to offer services at a compelling and competitive cost to attract millions of public safety users and make FirstNet self-sustaining. The use of FirstNet services and applications will be voluntary. The costs for FirstNet services and devices have not yet been set.

WIRELESS BROADBAND, DEDICATED TO PUBLIC SAFETY

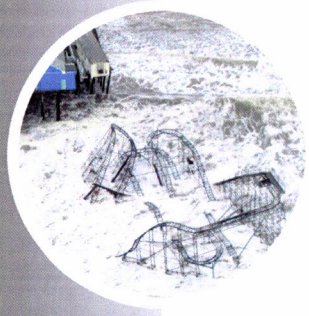
FirstNet™
U.S. DEPARTMENT OF COMMERCE

For more information contact: Kristi Wilde, Kristi.Wilde@firstnet.gov www.firstnet.gov

The Process for Working with FirstNet

State Consultation and Outreach

To make FirstNet a nationwide network, all states must have a radio access network (RAN) that connects to the FirstNet core. By law, FirstNet is responsible for working through the designated state point of contact to consult with states, local communities, tribal governments and first responders to gather requirements for developing its RAN deployment plan. These outreach efforts began in mid-May 2013 with six regional workshops. Ten individuals from each state/territory, including some tribal representatives, participated in an interactive meeting where they provided requirements, priorities and concerns to FirstNet. Now FirstNet is gearing up for individual visits to continue the dialog about our common mission.



State Visits

FirstNet will work through the designated state point of contact to arrange a visit, agree on the agenda and identify participants. Timing will depend on state readiness, the State and Local Implementation Grant Program (SLIGP) Phase 1 award and how quickly FirstNet can staff up its outreach team. The agenda for the initial FirstNet visit will focus on users and coverage needs, leveraging available information from the Department of Homeland Security Office of Emergency Communications. We will also discuss known state assets, expectations for data collection, as well as other state-specific issues. This meeting will pave the way for ongoing collaboration that will culminate in the development of a plan from FirstNet for constructing state RAN.

Tribal Outreach

FirstNet plans to create an education and outreach program to engage tribal members in discussions about the network and their public safety needs. FirstNet will encourage state governors to include tribal nations in the local FirstNet consultation process. In addition, FirstNet plans to hold separate meetings with tribes.

Data Collection

Data gathering, supported by funding from SLIGP Phase 2, will help ensure that the FirstNet state RAN build-out plans meet user needs. FirstNet will preview the components of the data request to help states understand the level of effort so they can adjust their SLIGP budgets accordingly. Data collection will cover the following general areas:

- Architecture of an evolved packet core and radio access network
- Required coverage areas of the network
- Hardening, security, reliability and resiliency requirements
- Assignment of priority users and selection of secondary users
- Availability of assets that may be utilized

States will be asked to submit available data as soon as it is compiled instead of waiting to complete the entire data request. FirstNet will continually update planning and modeling efforts based on new input. Our goal is to avoid surprises by working closely with state representatives as we develop the final FirstNet build-out plan.

RAN Proposal Response

To make FirstNet a nationwide network, all states must have a RAN that connects to the FirstNet core. A state can decide whether to have FirstNet construct the RAN or, it can "opt out" and seek the required approvals to build its own RAN that meets stringent FirstNet requirements.

RAN Response Timing

A state has 90 days from the date that the governor receives the FirstNet build-out plan to notify FirstNet, NTIA and the FCC in writing whether it prefers to engage FirstNet to build its RAN or construct its own RAN. If a state chooses to build its own RAN, it has 180 days to complete a request for proposal for its RAN. The state must also submit an alternate plan to the FCC for consideration.

State Decision Process

FirstNet will collaborate with states to develop and deliver a RAN plan that meets their needs.

Consultation
- Regional Workshops
- State Visits
- Ongoing Dialogue

RFP Process

FirstNet Presents Plan to Governor

State Decision
2 Options

90 days to decide and notify FirstNet, NTIA and the FCC

Opt Out

State seeks approval to construct its own RAN

State Requirements:
- Notify FirstNet, NTIA and the FCC of intention to build within 90 days of receiving FirstNet Plan
- Submit alternate plan to FCC and gain FCC approval
- Complete an RFP
- May apply for grant funding from NTIA
- Must apply to NTIA to lease FirstNet spectrum

Accept FirstNet Plan

FirstNet builds the RAN. FirstNet intends to cover the cost to construct, operate, maintain and improve the RAN.

Funding the Build-out

If the state's plan is approved by the FCC, the state may apply for grant funding from NTIA. To obtain federal funding to construct a RAN, a state must:

- Demonstrate the technical capability to operate and fund the RAN
- Maintain ongoing interoperability with the FirstNet network
- Complete the project within specified comparable timelines
- Execute its plan cost effectively
- Deliver security, coverage and quality of service comparable to the FirstNet network

There are additional funding implications if a state receives approval to build its own RAN:

- States pay any fees associated with using FirstNet core elements
- Grant program specifics are not developed yet
- NTIA will determine: eligible costs of the grant program; whether a match will be required; and funding levels

Licensing FirstNet Spectrum

If the state plan is not approved, the construction, operation and maintenance of the state RAN will proceed in accordance with the FirstNet plan. If a state receives approval to build its own RAN, the state then needs to negotiate a lease for the use of FirstNet spectrum.

WIRELESS BROADBAND, DEDICATED TO PUBLIC SAFETY

FirstNet™
U.S. DEPARTMENT OF COMMERCE

For more information contact: Kristi Wilde, Kristi.Wilde@firstnet.gov www.firstnet.gov

VIEW FROM THE TOP

Forward-looking perspectives from top leaders, regarding where our industry is today and, more importantly, where it is heading.

FirstNet invites participation in human-factors study that will be crucial to success

Aug. 12, 2013 by Urgent Communications contributor in View from the Top

FirstNet needs to understand how the new network will affect the way law-enforcement, fire and emergency-medical-services personnel carry out their duties every day. By considering human factors, FirstNet can design systems that fit the human body and its cognitive abilities, as well as optimize system performance and productivity.

By Harlin McEwen, chairman, Public Safety Advisory Committee (PSAC)

Much of the discussion about FirstNet—the nationwide, public-safety broadband network now in development—has focused on technology. However, an extremely important, but often overlooked, aspect of this network is the impact it will have on people. We need to understand how the new network will affect the way law-enforcement, fire and emergency-medical-services personnel carry out their duties every day.

FirstNet must consider human factors and design systems that fit the human body and its cognitive abilities, as well as optimize system performance and productivity. This is crucial in the public-safety environment, where split-second decisions and actions are often essential to save lives and property.

The FirstNet Board has asked the PSAC to analyze the long-range changes that the new network will have on people who use, operate and maintain the network every day. The PSAC believes that the needs of first responders and the individuals who support them, along with the latest technology, must drive network-design decisions.

When FirstNet is operational, public-safety agencies will have the ability to send data, video, images and text and make commercial-grade voice calls. Priority access and greater security and reliability will be key features of the network. These capabilities will provide dramatic improvements over the way we communicate today.

In our current land-mobile-radio environment, we have thousands of disparate wireless systems deployed by local, state and regional entities. The resulting interoperability problems extend across people, as well as technology.

For example, during Katrina and Sandy, public-safety personnel rushing from jurisdictions outside the affected areas to provide mutual aid often needed orientation to local communications terminology and practices. That can cost time, money and lives. With a nationwide network, we can remedy this situation. First, we must develop standardized approaches; then, individuals must be trained to use them. That's a tall order, but the benefits are well worth the effort.

The PSAC has enthusiastically tackled this assignment from the FirstNet board, and the PSAC executive committee has developed a template to gather data. The template has been distributed to PSAC members, and the plan is to deliver our recommendations to FirstNet this fall, so they can be included in the extensive market research that FirstNet is conducting prior to selecting network technologies.

The PSAC already has divided its initial research into four design categories: devices, applications, policies and procedures and network access/security. We will be investigating the ergonomic needs of users, operators and "maintainers"—those responsible for infrastructure maintenance—in each of these areas. Here are examples of these needs:

Devices

Police officers need devices that can be operated with one hand, and firefighters must use devices while wearing heavy gloves. Emergency medical technicians (EMTs) and paramedics require devices supporting concurrent video, voice and telemetry for transmitting patient data to emergency-room personnel. Network operators—FirstNet and any potential partners—must deliver priority-access capabilities for devices and applications and the ability to provision devices remotely. Those who maintain infrastructure day-to-day need the ability to authorize access to information resources on the fly and remotely activate/deactivate devices, components and applications without user intervention.

Applications

GPS and voice-enabled navigation applications providing turn-by-turn directions to incident scenes can be provided to users. Infrastructure elements must support end-to-end security for delivery and use of sensitive data, such as information from the National Crime Information Center (NCIC), Nlets—the international justice and public-safety network—and state criminal justice information systems. Maintainers want applications and data sources to incorporate criteria for authorizing use by local, regional, state, multistate and/or nationwide entities.

Policies and Procedures

Documentation, training and exercise doctrines must be developed for users working with new devices, applications and data sources. FirstNet will need to define and offer high availability, prioritization, quality-of-service (QoS), redundancy and resiliency.

In addition, memoranda of understanding and service-level agreements must be developed for operating partners, whether they are commercial or governmental entities. Maintainers will need operating procedures for the life cycle of devices, applications and data sources.

Access (Security)

One of the key ways that FirstNet will be differentiated from commercial networks is in the area of security. Ubiquitous, end-to-end authenticity and confidentiality of information traversing the network will be crucial for users, operators and maintainers.

There are many examples of excellence in specific public-safety agencies around the country. We will leverage this knowledge of human factors as we develop a nationwide vision and strategy. When FirstNet launches, we want to ensure that it works better than anything we have today for our emergency responders.

I invite *Urgent Communications* readers to provide their ideas and recommendations to their PSAC representative or directly to the PSAC at PSAC@hq.dhs.gov.

The law creating FirstNet required that its Board establish a standing Public Safety Advisory Committee to assist it in carrying out its duties and responsibilities. Harlin McEwen serves as chairman of this committee. He is also chairman of the communications and technology committee of the International Association of Chiefs of Police. Now retired, McEwen previously served as police chief for the city of Ithaca, N.Y., and as FBI deputy assistant director in Washington, D.C.

Public Safety Advisory Committee
Over the Horizon/Human Elements/Factors
Scoping and Data Gathering Template

Task Scope: The Public Safety Advisory Committee (PSAC) was asked by FirstNet to analyze the long-range impacts of the nationwide public safety broadband network (NPSBN) on the way law enforcement, fire, and EMS operate and consider the impact it will have on their duties once the network is built and operating. It is important that the business and needs of first responders drive decision, not technology. This task looks to answer the questions:

- What are the human elements that FirstNet needs to consider when designing the network?
- What are the potential user issues that will arise when using the NPSBN?
- How will the NPSBN be used by first responders and how will it impact operations?

To determine the human factors[1] impact of the network, the PSAC Executive Committee (EC) defined the "human element" of the system as users, operators[2], and maintainers[3]. Next, the PSAC EC identified categories to compartmentalize the various impacts, which are shown in the table below. Based on these categories, PSAC members are being asked to brainstorm and list potential human impacts. Examples are provided in *italics* for each category. Once PSAC members submit the initial list of impacts, the PSAC EC will compile and review the input and provide to FirstNet for review. The PSAC EC will then work with FirstNet to determine the highest priority categories and human factors/elements. Once the highest priority factors/elements are determined, the PSAC will develop recommendations or proposed processes outlining how these human elements should be addressed.

[1] Human factors is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and other methods to design in order to optimize human well-being and overall system performance.

[2] Operator is responsible for the day-to-day operations of the network (e.g., FirstNet, commercial carrier)

[3] Maintainer would be the entities/divisions within the operator entity that are responsible for maintenance services for the operator. Personnel that keep the day-to-day infrastructure elements running.

Category	Human Element Group		
	Users	**Operators**	**Maintainers**
Device design/ergonomics (detail public safety grade)	• *Police officers need the ability to use device with one hand* • *Fire fighters need the ability to use devices while wearing heavy gloves* • *EMT/Paramedics need devices that support concurrent video, voice and telemetry transmissions for patient to ER Doc teleconferences* • *Need ruggedized devices – able to withstand harsh environments (e.g. resistant to heat/cold, drop, dust, water, etc.)* • *Device hardware supports the collection of various biometric data from the user or others* • *Device supports integrated security platform when coupled with proper application(s) can securely receive/transmit TS classified materials* • *Devices incorporate power sources that provide a minimum of 10 hours duty cycles* • *Devices in all form factors shall support a secured common alerting protocol for one-to-one and one-to-many communications* • *Applicable devices should support the creation of ad hoc secured/non-secured WiFi personal area networks*	• *Devices may be provisioned remotely by local and nationwide operational entities* • *Device authorizations to information resources may be adjusted by competent authority "on the fly"* • *Device hardware supports Band 14 and commercial bands for interoperability* • *Infrastructure supports ample bandwidth availability for concurrent collection of various biometric data from the users or others* • *Infrastructure will support differentiation of priority access of devices and applications accessed upon devices*	• *Devices may be provisioned remotely by local and nationwide operational entities* • *Device authorizations to information resources may be adjusted by competent authority "on the fly"* • *The fault management system(s) and console controls shall allow remote manipulation of devices to activate/deactivate the device or components, and/or applications without user intervention*

Category	Human Element Group		
	Users	**Operators**	**Maintainers**
Applications	• *Applications support the collection, use, transmission, and receipt of multiple concurrent streams of biometric data* • *Applications support integrated security hardware platform that can securely receive/transmit TS classified materials* • *Applications incorporate Video Analytic capabilities* • *Applications integrate with and expand capabilities of connections to National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), State, Regional and local Criminal Justice Information Systems* • *Applications allow devices to access and control switched video sources at or enroute to incident scenes* • *Applications will provide GPS and voice-enabled navigation systems providing turn-by-turn directions to locations*	• *Infrastructure supports ample bandwidth availability for use, transmission, and receipt of multiple concurrent streams of biometric data* • *Infrastructure supports ample bandwidth availability for the use of Video Analytics* • *Infrastructure elements support the end-to-end provision of security elements supporting TS materials*	• *Applications incorporate criterion that articulate suitability and authorization/certification for use upon the network specifying local, county, multi-county, regional, state, multi-state, nationwide access or use.* • *Data sources should incorporate criterion that articulate suitability and authorization for use upon the network specifying local, county, multi-county, regional, state, multi-state, nationwide access.*

Category	Human Element Group		
	Users	**Operators**	**Maintainers**
Policies and Procedures	• *Training and exercise doctrine is developed supporting various device form factors* • *Training and exercise doctrine is developed supporting various applicable applications and data sources* • *Differential operational documentation developed regarding the behavior of devices and applications on FirstNet vice Commercial Networks if applicable*	• *Operating procedures and guidelines are developed for device, applications and access to various data sources* • *FirstNet and operators must define the required availability of the network in terms of availability = (total time – down time) / total time based upon the defined public safety need* • *The network will incorporate and utilize standardized elements that dictate prioritization and Quality of Service (QoS) attributes* • *Redundancy/Resiliency and high availability elements of the network must incorporate accepted practices of elimination of single points of failure, graceful and reliable failover between primary and secondary/backup elements or components and the prompt notification of failures* • *MOAs, MOUs, SLAs and/or contracts are developed between FirstNet and Commercial Carriers regarding the use of commercial networks or elements thereof by public safety users* • *MOAs, MOUs, SLAs and/or contracts are developed between FirstNet and Local, State, Regional, Federal and Tribal governments for the use of their networks, elements thereof or data by FirstNet public safety users*	• *Operating procedures and guidelines are maintained through a life-cycle process for applicable devices, applications and access to available data sources* • *The network must incorporate a comprehensive fault management system specifically focused for a high availability environment* • *Development of comprehensive doctrine for high availability environments* • *The network must take into off-network, peer-to-peer, and self-healing capabilities which are critically important*

Category	Human Element Group		
	Users	**Operators**	**Maintainers**
Access (security)	• *Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided*	• *Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided*	• *Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is consistently maintained*