AN APPROACH TO PROVIDE TACTICAL WIRELESS BROADBAND CAPABILITY IN AN AFFORDABLE AND SUSTAINABLE MANNER

Concept Behind:

"The DHS TACnet Program"

Developed By:

John Santo

DHS Joint Wireless Program Management Office

February 2012

EXECUTIVE SUMMARY

DHS Tactical Communications Land Mobile Radio (LMR) systems have exceeded their service-life and urgently need to be modernized to meet Federal and DHS mandates. DHS employs these LMR systems to provide voice communications, which are vital for successful missions and operations, and are essential for the safety of its agents and officers. Using available funding, DHS is modernizing these systems with newer systems that meet the mandates but continue to provide another generation of voice-only capability. Analysis shows that there is insufficient funding for DHS to continue modernization of its systems using the current approach at the pace needed to meet the growing operational need. Furthermore, initial projections show that billions of dollars and decades, at current funding levels, are required to upgrade and maintain these systems nationwide using the current approach.

This white paper describes an alternative approach to owning, operating, and maintaining stand-alone radio systems that provide a sustainable, cost-effective solution to meet DHS mission-critical wireless voice and data communication needs and is also applicable to Federal agencies and public safety entities. This approach proposes leveraging commercial networks to the maximum extent possible, thereby improving lifecycle costs, interoperability, and simplifying operation and maintenance. DHS is interested in assessing private industry's ability to meet DHS's requirements and assist in developing a roadmap with associated costs for implementation.

UNDERSTANDING THE PROBLEM

Today, DHS operates more than 20 private national radio networks serving more than 120,000 front-line agents and officers. Although these legacy networks provide critical voice communications that are essential for the safety of DHS agents and officers in effectively performing their missions and operations, most of these systems were deployed more than 20 years ago. They are well beyond their intended service life, do not provide sufficient coverage for agents and officers in remote locations, and do not meet Federal mandates for security (i.e., encryption) and efficiency (narrow-banding spectrum usage). As a case study, CBP alone has been upgrading these mission critical systems with an annual investment of $40M. Continuing at its current pace, CBP projects that modernization activity for the entire nation would take more than 20 years to complete with a capital investment of approximately $1.3B, not including lifecycle operations and maintenance costs.

The current modernization approach replaces analog LMR with new standards-based digital LMR systems, which continue to provide similar voice-only capability. Unfortunately, this approach does little to support a growing need for mission-critical data like full motion video, sensor data, still-images, biometric information, and location-based situational awareness sought by DHS, public safety, and Federal agencies. Across the nation, public safety and law enforcement agencies are driving towards the use of wireless broadband systems to provide their end-users with new integrated voice and high-speed data capabilities to improve efficiency and effectiveness in missions and operations. The DHS Joint Wireless Program Office believes that wireless broadband systems, if implemented by DHS and the homeland security and public safety community, could yield substantial cost-savings and increase functionality, coverage, and capacity in direct support of the various missions and operations.

DRIVERS FOR CHANGE

The key objectives for changing the current modernization approach are reducing costs and time to deploy, satisfying a critical need for data and broadband access in the field, improved interoperability, reducing complexities for end-users, and increased spectrum efficiency. Each of these objectives is discussed in further detail below.

Unsustainable Cost and Protracted Deployment Schedule

The traditional approach utilized for several decades across the broad public safety community has been to deploy many overlapping, privately-owned and operated systems, each serving small user communities with maximum customization and with many proprietary features. The annual costs of owning, operating, and maintaining these private systems is extremely expensive and DHS does not see this model as financially sustainable into the future. Because the LMR technology serves a small mobility market segment, the costs associated with refreshing these systems at the end of their lifecycle is exorbitant and does not gain cost efficiencies from the large global commercial mobility market proliferation underway. According to DHS estimates, if we remain on another product cycle generation of private LMR technology, a $3.2B investment is needed just to upgrade and modernize existing end-of-life tactical communications systems Department-wide with only 15 percent of this requirement funded at the current time. The large capital and operating cost investments over a long deployment period and the absence of dedicated funding to build, own, operate, and maintain private systems makes the current approach unsustainable for the future. Additionally, keeping current systems operational using the limited or foreseeable available funding keeps DHS from focusing on the emerging needs for broadband wireless technology. DHS and Federal agencies require a viable alternative that is affordable and sustainable.

Expected Use of Broadband Services

DHS is experiencing a growing demand from its operational components for mission-critical voice, data, video, and applications that require the end-user to have mobile broadband. DHS has documented these user needs in a Joint Mission Needs Statement and is developing the Concept of Operations and Operational Requirements Documents. As seen in the commercial markets, the proliferation of commercial broadband cellular access in the consumer market has led to the rapid introduction of many new mobile smart devices and a seemingly endless rollout of mobile applications to run on these devices. Our homeland security and public safety communities have, for the most part, not systematically incorporated these powerful

tools in their operations due to the need for enhanced security, always available reliability, and survivability in mission critical communications.

Increased User Complexity

Instead of building smarter networks that are easier for end-users to operate, the voice-only LMR systems currently being deployed at DHS are increasingly more complicated and difficult to use. For example, today's LMR radios have more than 500 channels, with more than 1000 programmable options in each radio. There is a heightened risk of user error and the need to perform manual functions that are typically handled by the network in modern commercial systems. Preventing these errors requires devoting many hours to training, time which can otherwise be directed toward operations. Additional complexities result because many of these radios cannot be configured and updated over the wireless network, requiring that they be temporarily removed from service and reprogrammed by trained technicians, physically touching the radios and then redeployed. To achieve the desired efficiencies and improvements in performance of its missions and operations, DHS should undertake a modernization strategy that removes or minimizes complexities from its operational end-users and leverages smart networks and technologies.

Spectrum

A nationwide modernization of DHS's LMR network using modern LMR technologies requires a significant number of dedicated radio frequency channels in the Federal Very High Frequency (VHF) LMR band. Because of the scarcity of available channels coupled with the prevalence of Federal communications systems that currently operate or plan to operate in this spectrum band, DHS faces a risk of not having enough channels to deploy the required system capacity and design. This lack of available spectrum makes it even more difficult when deploying new LMR systems along the borders since DHS must compete for frequencies with neighboring countries in addition to other Federal agencies. If spectrum is not available, then DHS will not be able to provide coverage at those locations.

Furthermore, spectrum is becoming scarcer as commercial, public, and public safety wireless demand increases. Projections from both the White House and Congress indicate that this trend will sharply increase over the next decade which, in turn, puts increased pressure on the Federal government to repurpose prime spectrum for the greater public good. Recently, the White House signed a memorandum to free up about 500 MHz of spectrum for commercial and public use. Legislation is also being proposed[1] seeking spectrum to foster further build-out of commercial wireless services. These trends suggest that Federal agencies are unlikely to acquire the necessary spectrum to continue deployment of traditional LMR systems using the current inefficient private network approach. In fact, Federal agencies are more likely to lose some spectrum if they cannot justify a compelling need for it or demonstrate that it is being used efficiently. These pressures are too great for Federal agencies to ignore. The risk of being forced to give up spectrum and forced to move to suboptimal solutions because of a failure to adequately plan for this likelihood would negatively impact missions and operations. To prepare for this risk, next generation mission critical communications solutions must reduce the need for dedicated LMR spectrum and move in a common direction with commercial broadband innovation, where increases in spectrum are likely to occur. DHS and other Federal agencies should also promote the development and use of a National Public Safety Broadband network that would leverage public safety spectrum in a more efficient manner.

Impediments to Interoperability

DHS needs interoperable communications with Federal, state, local, tribal, and international partners to effectively conduct its missions and operations. Legacy LMR technologies present many challenges to achieving this interoperability due to technical, operational, and policy issues. Two main issues that obstruct interoperability are the use of hundreds of private, stove-pipe systems, developed using different frequency bands and customized with the use of many proprietary features and equipment. For example, many state, local, and tribal agencies use 800 MHz radios while Federal agencies use VHF or UHF radios. Standard LMR radios cannot be used to communicate across these frequency bands. Interoperability is further complicated by the fact that many public safety end-users are migrating to broadband systems[2] in the 700 MHz band while DHS and other Federal agencies continue to build and operate systems in the VHF and UHF LMR bands. Although there have been recent attempts to solve these problems with multi-band radios and P-25 standards, these solutions focus on the subscriber radio and continue to increase complexity for operational end-users, do not reduce escalating infrastructure costs associated with owning and operating private mobile networks and do not address broadband emerging user requirements. An effective approach must be affordable, easy to use, and improve interoperability, ensuring effective communication between DHS and its partners.

PROPOSED APPROACH

This section describes the proposed modernization approach that would provide broadband capabilities including voice and data applications while reducing costs, reducing deployment time, improving interoperability, and simplifying operations and maintenance.

New Subscriber Devices Enable Broadband

Today, many public safety agencies are contemplating building, owning, and operating two separate, privately-owned national

[1] H.R. 3125: Radio Spectrum Inventory Act requires an inventory of the radio spectrum bands management by the National Telecommunications and Information Administration and the Federal Communications Commission

[2] FCC has granted conditional waivers to 21 regional and local entities to begin building wireless broadband networks for Public Safety first responders.

networks -- one delivering narrow-band LMR voice and another delivering broadband high speed data processing, video, and high resolution imaging. If instead of using this two network approach, technology became available to enable ***converging*** full functionality of LMR voice along with broadband data and video applications on a single network, this would significantly reduce cost. Many innovations could accomplish this, such as; an LMR radios with an embedded wireless broadband chip, a card slot, or a USB slot similar to a laptop computer; sleeves or adapters that attached to our inventory of existing LMR radios to enable wireless broadband access. These radios (or existing radios with adapters) would have two modes of operation: (1) traditional LMR operation using current dedicated DHS spectrum and legacy LMR systems, and (2) commercial/public safety broadband operation for communication extending beyond the immediate local area. This approach allows direct LMR radio-to-radio communication on current LMR frequencies and voice only LMR networks and also allows the routing of LMR traffic as an application over available broadband networks to communicate to a wide areas talkgroup, dispatch or a communication center. Another benefit of this approach is that use of these LMR radios would enable seamless transition from the "as is" state (i.e., LMR based infrastructure) to the future converged broadband vision.

Based upon mission needs and user requirements, an end-user could select one or more public safety grade devices (e.g., LMR radio, standard mobile data terminals, laptops, Smart Phones, or Personal Data Assistants (PDA)). It is envisioned that these devices would be similar to those used by the consumers (gaining the scale of efficiency in chipsets and interface standards from the global mobility device market) but specially configured for public safety applications. All devices would be capable of communicating over commercial standard broadband wireless infrastructure, with DHS OneNet as the single core wired IP transport infrastructure.

Costs of Ownership and Deployment Schedule

DHS's vision is to leverage existing commercial and private networks to the maximum extent possible and not to build and own networks. The funding model could require a one-time investment for service installation followed by a monthly subscription fee, significantly reducing capital investment. These monthly operating costs would be less when compared to the privately-owned and operated model because the network operating costs are shared among public customers and other public safety end-users. Some of these monthly costs are already incurred with existing commercial mobile wireless services. By aligning with commercial broadband wireless service evolution, additional cost savings would be realized by not having to continually upgrade infrastructure as broadband speeds continue to evolve at a rapid pace. DHS could gain the benefits of all commercial infrastructure upgrades, without needing to make large capital investments.

Leveraging existing commercial technologies enables DHS to leap-frog from voice-only capabilities to available broadband capabilities addressing the voice, video, imaging, situational awareness, and in-field processing requirements. In some cases, large state and local agencies are deploying or plan to deploy broadband infrastructure, in accordance with the FCC National Broadband Plan, for public safety shared use. DHS's approach would leverage these public safety networks wherever they exist. Taking advantage of existing public safety broadband and commercial broadband infrastructures would result in significant reduction in cost and deployment roll out schedules.

However, use of commercial and public safety infrastructures requires a network integrator to interconnect commercial and private broadband networks into a virtual single network. This will enable the user to seamlessly roam across these networks in a transparent manner as if it was a single network. This integrator must also fill in gaps where commercial network service does not exist. DHS or the Federal government may have to subsidize the building of these gap areas. (The costs associated with just building the gap areas would be significantly less than building and owning networks covering the entire nation.) Also, by using the one-time installation followed by recurring subscription cost model, the integrator would leverage costs across a larger community than just DHS.

Network Hardening

To meet DHS (or public safety) needs, these networks must be optimized to meet a higher grade of service. Specifically, the networks must provide for priority access to assure that DHS can access the network even during high demand. To ensure that DHS traffic is safeguarded, the network must support encryption based on DHS standards. Finally, DHS voice traffic must be carried with high reliability and minimum delays. This Mobile Virtual Private Network description is similar to Virtual Private Network technology used today on wired IP networks. The network integrator must develop the capability to meet this higher level standard of security and service.

Interoperability and User Complexity

Interoperability will be achieved through standards-based commercial technologies and networks.. For example, commercial end-users today can communicate with each other regardless of technology or the carrier (i.e., AT&T end-users can communicate with Verizon, T-Mobile, and Sprint end-users). This level of interoperability is achieved through the use of modern networking technologies and commercial wireless standards.

To promote interoperability even further, DHS plans on developing a National Interoperable Communications Center (NICC) which will house central servers that will:

- Manage (establish and maintain) talk groups and membership (both LMR and broadband) based on mission requirements;
- Manage encryption to ensure end-users can communicate with each other securely, and;
- Configure and reprogram radios by pushing updated configurations and programming of radios over broadband networks

Reduced end-user complexity will result from centralizing and remotely managing the end-users' devices, talk groups, and encryption (i.e., keys). In addition to having direct interoperability channels for partners requiring frequent and routine interoperability, it is expected that when end-users require interoperability services beyond the normal they will make a radio request to the NICC. Upon receipt of the request, the NICC will establish a dynamic talk group and add required or requested end-users and associated resources (e.g., radio channels). When this talk group is no longer required, the NICC will disband the talk group along with all associated resources. This will greatly reduce the complexity and radio congestion for operational end-users.

Spectrum Efficiency

Spectrum efficiency would be achieved through the use of commercial or private networks to transport voice and data traffic. If large-scale, high bandwidth, fully integrated networks such as those being proposed by the FCC, Congress, and the current Administration become reality, they have the potential to meet the emerging demands of DHS and the entire public safety community for many years. Modern packet-based networking technology and functional integration greatly improves spectrum efficiency and moves Federal agencies along a common modernization path with commercial technology evolution.

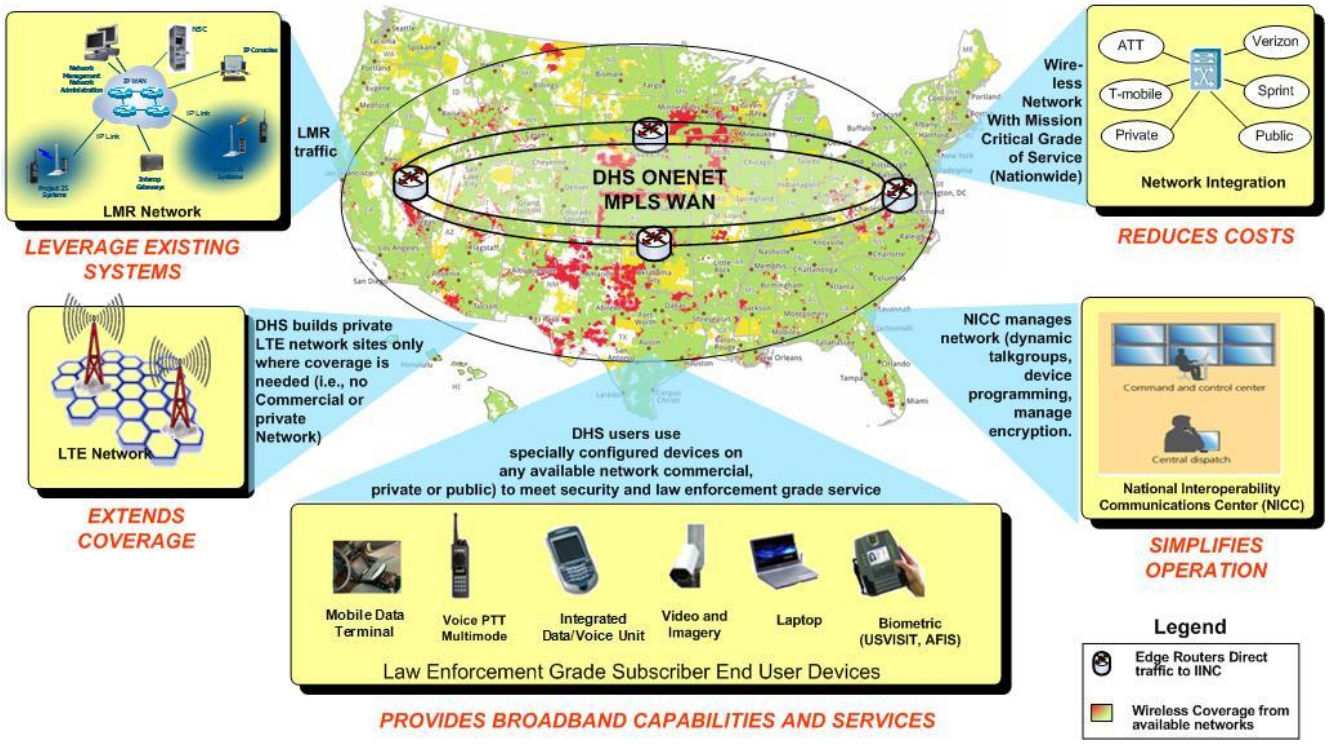
NEED FOR SEEKING INDUSTRY INNOVATION

There is a need to work with industry to understand how to achieve this new approach. Areas that must be better understood include:

- Reducing development and deployment risks;
- Fostering private industry interest and solution competition;
- Promoting cost savings efficiencies and shifting the budget allocation paradigm from massive capital expenditures towards straight operational expenditures;
- Aggregating the public safety need into a larger market segment (than current individual agencies with customized designs) and aligning with new public safety broadband legislative actions, and;

SUMMARY

This white paper offers an alternative approach that would bring tactical wireless broadband capabilities to the end-user in a sustainable, cost-effective, and timely manner. This proposed modernization approach appropriately leverages public safety networks where and when available, commercial networks to the maximum extent possible, improves coverage, enhances interoperability, and simplifies operation. Innovation research and development is immediately needed to assess the ability of private industry to implement solutions based on this proposed approach.


LMR Network
LMR traffic
LEVERAGE EXISTING SYSTEMS
DHS ONENET MPLS WAN
Wire-less Network With Mission Critical Grade of Service (Nationwide)
ATT
Verizon
T-mobile
Sprint
Private
Public
Network Integration
REDUCES COSTS
LTE Network
DHS builds private LTE network sites only where coverage is needed (i.e., no Commercial or private Network)
EXTENDS COVERAGE
NICC manages network (dynamic talkgroups, device programming, manage encryption.
Command and control center
Central dispatch
National Interoperability Communications Center (NICC)
SIMPLIFIES OPERATION
DHS users use specially configured devices on any available network commercial, private or public) to meet security and law enforcement grade service
Mobile Data Terminal
Voice PTT Multimode
Integrated Data/Voice Unit
Video and Imagery
Laptop
Biometric (USVISIT, AFIS)
Law Enforcement Grade Subscriber End User Devices
PROVIDES BROADBAND CAPABILITIES AND SERVICES
Legend
Edge Routers Direct traffic to IINC
Wireless Coverage from available networks