Before the Department of Commerce

National Institute of Standards and Technology

325 Broadway, Boulder, Colorado 80305

Re: Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network, Notice and Request for Comment, Docket No.: [110727437-1433-01]

Comments of Harris Corporation

The Harris Corporation (Harris) hereby submits these comments in the above-referenced proceeding,[1] and lauds the National Institute of Standards and Technology (NIST) for its ongoing efforts to ensure successful deployment of a nationwide interoperable public safety broadband wireless network (PSWBN).

THE HARRIS CORPORATION

Harris is an international communications and information technology company serving government and commercial markets in more than 150 countries. Headquartered in Melbourne, Florida, the company has approximately $6 billion of annual revenue and more than 16,000 employees — including nearly 7,000 engineers and scientists. Harris is a leading global supplier of secure radio communications products and systems, and embedded high-grade encryption software, for the military, government, and public safety. Harris is a pioneer in the development of internet protocol (IP) based networks for private radio and broadband applications, and supplies industry-leading narrowband, multiband, and broadband networks, services, and devices. Harris' Chief Technology Officer for RF Communications Division, Dennis Martinez, Chairs the FCC's Emergency Response Interoperability Center (ERIC) Public Safety Advisory Committee (PSAC) Security and Authentication Work Group.

[1] Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network, Notice and Request for Comment, Docket No.: [110727437-1433-01] (RFC).

Executive Summary

This document provides input to the Department of Commerce (DoC), National Institute of Standards and Technology (NIST) on the topic of the emerging public safety broadband network. It provides input on four key themes:

1. Resiliency During Emergency Response
2. Reliability & Availability
3. Cyber Security
4. Affordability and Commercial Alignment

For each of these themes, input is provided on the following:

- The importance of related features
- Current gaps that exist preventing the realization of the full potential of each feature
- Possible research and development that could close technical gaps
- Challenges that public safety could face in realizing the full potential of the feature
- Best practices from other industries that could be leveraged

This document also provides input into five additional topics:

1. Open Standards and Commonality
2. Multi-Vendor Environments
3. Affordability
4. Leveraging a Survivable Core & Cyber Infrastructure
5. Industry Engagement

Background

The advent of wireless broadband technology has been one of the most significant technology breakthroughs since 9/11. Backed by a vast global commercial eco-system, this industry is shaping every facet of our lives, and will drive social and economic change around the world. Smartphones and applications that operate on current and emerging wireless broadband networks are rapidly re-defining the information age in which we now live.

Regulatory policy in the U.S. has now paved the way for this exciting technology to be made available to our nation's first responders and others charged with protecting life and property of our citizens. Allocation of spectrum and funding are central to making the Public Safety Wireless Broadband Network (PSWBN) a reality. With the goal of achieving nation-wide interoperability, the issue of governance and network architecture are rightfully at the forefront of the ongoing dialog between policy makers, public safety organizations and the industry partners that support them.

NIST has properly recognized that there are unique requirements for the PSWBN that differ from commercially deployed networks. Although much of the foundational technology and commercial standards can and will be leveraged, there are key differences in the business model that drives public safety communication vs. the commercial business model that addresses the needs of consumers, business and industrial users. Consistent with the public safety mission, the need is to provide communication capabilities to first responders when and where they are called upon to protect life and property, and to do so while providing for their own personal safety.

Through a series of rule-making initiatives, and with virtual unanimous support, the FCC has mandated use of the Long Term Evolution (LTE) standard for the PSWBN. This is one of several steps that are vital to ensuring the PSWBN achieves the goal of nation-wide interoperability.

On September 7, 2011, members of the Visiting Committee on Advanced Technology (VCAT) Subcommittee on the National Public Safety Broadband Network and other stakeholders met to discuss prior work led by DoC/NIST. Harris participated in that meeting, and believes that a key outcome was a depiction of relevant technology and standards, which we illustrate below in Figure 1:

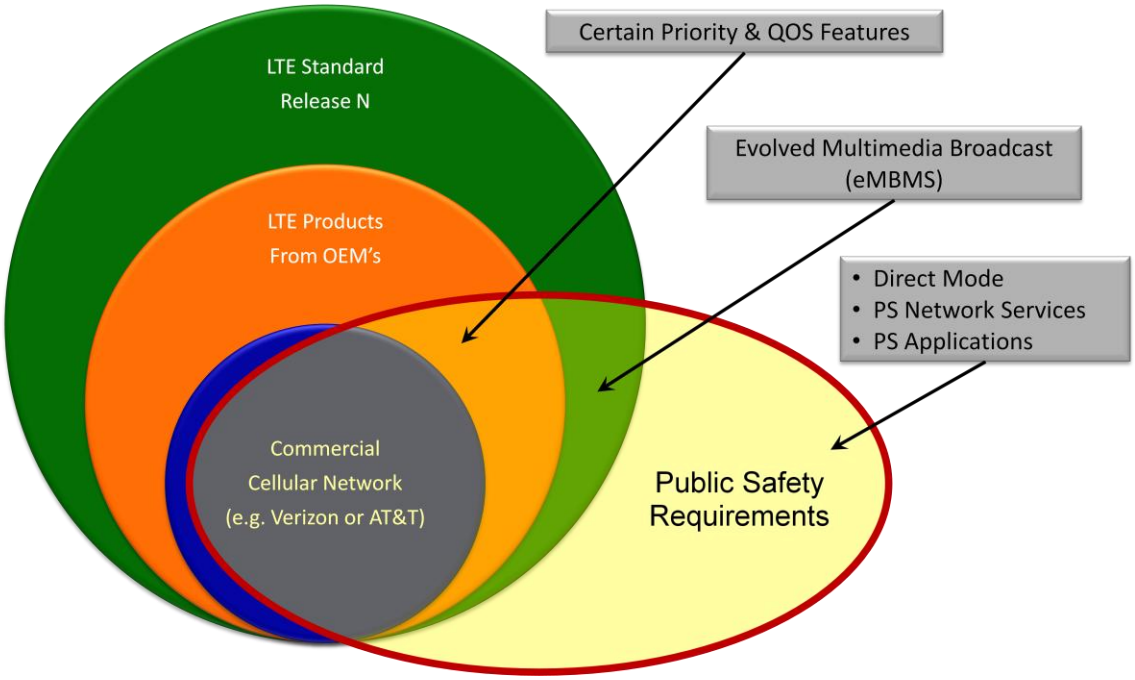


Figure 1: PSWBN Standards & Technologies

The LTE standard (depicted as the green circle), developed by the Third Generation Partnership Project (3GPP), is a comprehensive standard that evolves through a series of Releases. Original Equipment Manufacturers (OEM's) typically implement a subset of the entire standard (depicted by the orange circle), consistent of the market needs of commercial cellular operators, their primary market.

In turn, commercial cellular network operators deploy their networks on a further subset (depicted by the blue circle), reflecting their business models and targeted capabilities for their networks. As an example, certain priority and Quality of Service (QOS) capabilities are available in some OEM equipment, but these capabilities frequently are not implemented by commercial network operators, who primarily implement best-effort services, consistent with the needs of consumers that share network resources.

Finally, we note that public safety requirements overlap capabilities defined in the LTE standards (depicted by the yellow oval), implemented by OEM's and deployed in commercial cellular operators, and in some cases extend beyond. For example, one of the key requirements for public safety is off-network operation, sometimes referred to as Direct Mode or Talk-Around. This capability is not presently defined in the LTE standards. In similar vein, certain public safety network services and applications lie outside the scope of the LTE standards.

This illustration only addresses capabilities that broadly can be characterized by form/function/feature. There are also key operational and deployment differences between commercial networks and the PSWBN. As was noted and consistently emphasized by public safety practitioners in the August 2010 Department of Justice

Community Oriented Policing Services (COPS) National Forum on Public Safety Broadband Needs, resiliency and availability/reliability ranked high as critical requirements.[2] These needs are consistently in the forefront of requirements for currently deployed public safety networks. While there are technological aspects to these requirements, not to be overlooked are design and deployment practices due to fundamental differences between networks designed to serve consumers vs. networks designed for use by first responders and other public safety personnel. Commercial network design and deployment practices are based primarily around economic business models, as contrasted with public safety design and deployment practices that are based on the need to ensure communication anywhere, anytime and under the worst of conditions.

At this juncture, it is appropriate to briefly discuss two aspects of the commercial business model that serve as best practices. Commercial operators implement networks in accordance with their business objectives. The features, functions, and services they choose to implement are aligned with those business objectives. We refer to the selected features, functions and services as the operator's Network Profile, which as noted earlier is based on a selected subset of the particular standards it is based on, in this case LTE. Operators design, implement and test the products that comprise their network in accordance with their Network Profile.

Procurement of the products that are used to build their network, both infrastructure and user devices, are specified in accordance with the Network Profile. Interoperability Testing (IOT) is based on the technical elements defined in the Network Profile. The prevailing highly successful procurement practice is multi-sourcing, in which multiple vendors are selected for both infrastructure elements and user devices. Multi-sourcing is essential to commercial operators as a means to ensure a robust supply chain. Multi-sourcing drives affordability and innovation, in addition to ensuring un-interrupted source of products and services. These concepts are developed further in subsequent sections of this document.

Harris believes that translating these commercial best practices to the PSWBN should start with the definition of the PSWBN Network Profile. NIST has a key role to play, working together with public safety practitioners, organizations that represent public safety interests, OEM's, commercial network operators and technology specialists to define the PSWBN Network Profile.

---

[2] http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf

Resiliency During Emergency Response

Central to the mission of our nation's first responders are the functions they perform during emergency response as part of our 911 system, and during large scale events, both man-made and natural disasters. It is during these events that resilient communication networks are most vital. For this reason, public safety networks are deployed with significant redundancy, fault tolerance, and backup mechanisms to maximize the likelihood of proper operation for first responders while providing emergency response.

The Federal Communications Commission (FCC), Public Safety and Homeland Security Bureau (PSHSB) defines resiliency as:

> *"Resiliency refers to the ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements. Encompassing the technical aspects as well as the end-user information exchange aspects of interoperable communications, resiliency insures that the interoperability of communications systems is not affected by known or unknown circumstances of change. Resiliency also refers to the ability of the system to evolve and advance as new technologies or capabilities are developed. Furthermore, resiliency is a reflection of the flexibility of the system to respond to changes in operational requirements or implementation strategies and technologies."*[3]

On this theme, NIST seeks input on four functions. Assessment and recommendations for this theme are provided in Table 1.

Table 1: Assessment – Resiliency During Emergency Response

	Importance	Gaps	Possible R&D	Challenges	Best Practices
Resiliency The ability of operable systems to recover from mishap, change, misfortune or variation in mission or operating requirements	High	Rapidly deployable infrastructure and off-network operation	Last mile highly resilient backhaul networks and devices that support off-network operation	Backhaul networks capable of broadband data rates with full resiliency. Standards and spectrum for off-network operation.	Hardened shelters and towers, backup power sources Public safety radios implement Direct Mode allowing off-network operation

[3] http://publicsafety.fcc.gov/pshs/clearinghouse/core-concepts/resiliency.htm

Table 1: Assessment – Resiliency During Emergency Response					
	Importance	**Gaps**	**Possible R&D**	**Challenges**	**Best Practices**
Self Organizing Dynamically managing configuration by automatically making changes to ensure messages reach their destination	High	Commercial use cases may not align with emergency response use cases	Adapting LTE Self Organizing & Optimizing technologies to public safety use cases, in particular for emergency network optimization	Ease of use and dealing with sector capacity for high density use cases	Rules based Self Organizing Network (SON) management Cells on wheels
Meshing Each node serves as a relay for other nodes. Nodes are typically user devices.	Medium	Performance of mesh networks varies with node density	Investigate use of Mobile Ad-hoc Network (MANET) technologies used in military applications	MANET technologies may require additional spectrum for licensed operation	Use of WLAN technologies to support ad-hoc networking
Adaptability Ability of a network or device to modify/change behavior based upon external conditions	Medium	Establishing criteria and metrics that determine how adaptation works in practice	Applicability of cognitive radio	Ensuring adaptability mechanisms do not interfere with desired communications	Software defined radios

Reliability & Availability

Whereas resiliency speaks to functional operation of a network during emergency response, reliability and availability speak to grade of service for a network that is functioning properly, perhaps under severe or stressed loading conditions. On this theme, NIST seeks input on two functions. Assessment and recommendations for this theme are provided in Table 2.

Table 2: Assessment - Reliability & Availability

	Importance	Gaps	Possible R&D	Challenges	Best Practices
Prioritization The ability to prioritize network traffic based on assigned priority schemes	High	Current commercial networks do not implement prioritization schemes	Analyze LTE standards and system architectures to ensure scenario-based prioritization can be implemented	Commercial LTE OEM's may not support prioritization schemes consistent with public safety use cases	Modern trunked radio systems implement multiple layers of priority that enable users operating in emergency scenarios to receive priority access to communication resources
Quality of Service (QoS) Providing preferential delivery service for applications that require particular data throughput, latency, and/or jitter performance levels	High	Implementation of QoS in commercial networks is limited	Analyze LTE standards and system architectures to ensure scenario-based QoS can be implemented	Commercial LTE OEM's may not support QoS schemes consistent with public safety use cases. QoS needs to be extended beyond the Radio Access Layer, to ensure end-to-end QoS for applications that require it.	Commercial IP based QoS technologies are widely available. The LTE standard defines many QoS capabilities.

Cyber Security

Harris recommends that NIST consider a broader perspective on cyber security than is articulated in its Notice and Request for Comment. There are two distinct elements to cyber security. One is to protect the PSWBN from malicious attacks that would hinder or disrupt access to or use of this network. The other is to protect sensitive information and identities from compromise.

Recognizing the gravity of this issue, the FCC Emergency Response Interoperability Center (ERIC), Public Safety Advisory Committee (PSAC) formed a workgroup to provide recommendations on the topic of Security and Authentication (S&A WG). From that report:[4]

> *The importance of cyber security to the nationwide interoperable Public Safety Wireless Broadband Network (PSWBN) must be recognized and adequately addressed. Given the significant role of the PSWBN to provide a comprehensive communications capability to our nation's first responders and government organizations chartered to protect life and property, protecting this national asset must be a high priority. A comprehensive Security Architecture, which includes technology, policies and procedures, must be implemented to ensure protection of the PSWBN from malicious attacks in the face of evolving cyber threats and to protect information and identities from compromise.*
>
> *Widespread worldwide use of LTE technology and the deployment of numerous LTE-based networks will also make these networks a frequent target of cyber attacks. It is reasonable to expect the sophistication, frequency and resolve of these attacks to increase over time. It therefore becomes a prime consideration in constructing our nation's public safety broadband network to provide for its cyber security from the onset and throughout its life. Because of its particular mission, it is also reasonable to expect aggressive cyber attacks on the PSWBN will occur by those hoping to exploit vulnerabilities in order to compromise network availability or access information and/or identities for malicious purposes. The S&A WG agrees with comments provided by Northrop Grumman, "the use of open and globally deployed standards, such as Internet Protocol (IP) that forms the core of the LTE-based public safety broadband wireless networks, considerably increases the vulnerability of these networks to malicious attacks, further underscoring the need for robust security mechanisms to protect these networks". To that end, the Commission has properly recognized the need to protect this strategic asset along with the information and services it conveys. The S&A WG also notes that the Commission has on-going work on the topic of*

[4] Emergency Response Interoperability Center, Public Safety Advisory Committee (PSAC), Considerations and Recommendations for Security and Authentication, Security and Authentication Subcommittee Report, May 2011.

Cyber Security Best Practices. That body of work provides very broad recommendations of direct relevance to the PSWBN.

Local public safety agencies are also governed by several federal laws as related to security. These federal laws are further driving forces requiring a robust security scheme. The two major ones are the Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS). HIPPA covers the privacy and security of medical records. First responder emergency medical services personnel will need to use applications and devices which can recognize and conform to HIPPA requirements. CJIS has mandates and guidelines for limiting access to criminal justice information, widely used by law enforcement practitioners.

The PSAC S&A WG report also identified a list of key objectives for the security architecture for the PSWBN:

Table 3: Key Objectives for the PSWBN Security Architecture

Availability	Ensure that network services are not disrupted by malicious attacks
Privacy:	Ensure protection and integrity of sensitive data and identities
Interoperability:	Ensure that security mechanisms do not inhibit interoperability
Usability:	Ensure that security-enabled devices and services are easy to use
Quality of Service: QoS	Ensure that security mechanisms are not detrimental to achieving QoS required for mission critical applications
Cost Effective:	Ensure that the cost of implementing security is consistent with the cost associated with security breach
Standards Based:	Ensure robust standards are used for implementing the PSWBN Security Architecture
Flexibility:	Ensure that security can be tailored to support role-based security and allow local control and management of security, consistent with the over-arching security policy

On this theme, NIST seeks input on one function. Assessment and recommendations for this theme are provided in Table 4.

Table 4: Assessment - Cyber Security					
	Importance	**Gaps**	**Possible R&D**	**Challenges**	**Best Practices**
Strong, Dynamic Access Control Provide access control to network traffic and authenticate users/devices on the network	High	A comprehensive cyber-security system must be implemented in the PSWBN	Participation in implementation of a structured cyber security system, including: • Risk Assessment • Threat Assessment • Vulnerability Analysis Assess viability of survivable core – cyber infrastructure	Cyber threats will continue to evolve and become ever-more aggressive	• FIPS-140 • ITU-T X.805 • RSA SecurID, smart cards • X.509v3 user certificates • RADIUS-EAP (Extensible Authentication Protocol) • Public Key Infrastructure (PKI)

Affordability and Commercial Alignment

There will be significant benefit by commercial alignment between the PSWBN and commercial broadband networks. Indeed, use of commercial broadband networks by public safety agencies is highly prevalent today. At the same time, there is appropriate caution in the use of commercial off-the-shelf technology. Public safety practitioners have made a strong case for significant investment in the PSWBN, a purpose-built network using dedicated spectrum. While commercial networks provide an interim capability today, in the long term the PSWBN will be the primary network for advanced broadband capabilities that are "public safety grade" and tailored for the public safety mission.

One area of concern is that the PSWBN will likely support applications that may not run properly on commercial broadband networks – most notably when unique capabilities such as QoS or eMBMS are required. It is important to ensure that proper education and expectations are set for first responders that will eventually encounter this situation.

On this theme, NIST seeks input on seven functions. Assessment and recommendations for this theme are provided in Table 5.

Table 5: Assessment – Affordability and Commercial Alignment

	Importance	Gaps	Possible R&D	Challenges	Best Practices
Compatibility with Commercial Infrastructure Utilization of commercial services when public safety users are in locations not covered by the PSWBN	High	Commercial networks will not implement the full capabilities of the PSWBN	Development of application frameworks that mitigate the impact of differences between the PSWBN and commercial networks	Preventing users from being frustrated by differences in application function and performance between the PSWBN and commercial networks	PTCRB testing for device IOT across carrier networks Session persistence middleware as part of a Virtual Private Network (VPN)
Network Sharing Shared use of infrastructure between commercial networks and the PSWBN	Medium	Commercial infrastructure may not be implemented or deployed in accordance with public safety requirements or best practices	Reliability analysis & impact studies of shared infrastructure	Use of shared infrastructure must not compromise resiliency, reliability or availability of the PSWBN	Current public safety LMR systems occasionally make use of shared tower resources with commercial networks

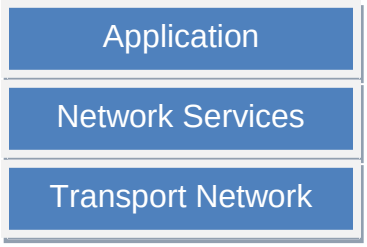
Table 5: Assessment – Affordability and Commercial Alignment					
	Importance	**Gaps**	**Possible R&D**	**Challenges**	**Best Practices**
Multi-Modal The ability of the network to support voice, video, data and multimedia simultaneously	High	The one-to-many model common in public safety will require implementation of advanced LTE capabilities such as eMBMS	Development of standards for utilizing eMBMS capabilities to implement public safety capabilities & services	Commercial network operators are not driving the implementation of eMBMS in their networks	For some use cases, IMS coupled with eMBMS can provide a standardized framework
Scalability The ability for the PSWBN to handle increasing load in a graceful manner, its ability to be expanded to accommodate that growth – this includes supporting a rapid increase in user loading in limited geographic areas	High	The PSWBN will likely be implemented over many years. It is imperative that the incremental approach to implementation enable scalability to ensure nationwide interoperability.	Architecture trade studies & assessment to ensure incremental construction of the PSWBN does not hinder its ability to scale. Application of LTE SON technologies to perform dynamic load balancing during peak events.	Maintaining a balance between ensuring nation-wide interoperability and the ability to provide flexibility to accommodate unique state & local requirements	Commercial network operators have many best practices to ensure continued evolution and incremental build out of their networks. Self Organizing Network (SON) capabilities that enable Self Optimizing
Power Awareness The ability of network and/or devices to control power functions	Medium	Commercial Smartphone devices may not be compatible with battery requirements for one or more work shifts common in public safety	Battery technology & power management strategies	Public safety devices may diverge from commercial devices in battery technology and power management schemes	Power management continues to be a significant investment focus in the commercial eco-system

Table 5: Assessment – Affordability and Commercial Alignment					
	Importance	**Gaps**	**Possible R&D**	**Challenges**	**Best Practices**
Standardized Common Interfaces Protocols, Application Program Interfaces, application platforms, radio capabilities, etc. that allow for competitive provisioning	High	LTE standards apply to the transport network and not to the network services and applications that are unique to public safety	Development of public safety network services that form the basis for interoperable applications	There are no standards bodies today that are ideally suited to defining public safety standards for applications	Commercial application paradigms such as IMS or Open Mobile Alliance (OMA) could serve as a model for public safety
Uniform, Universal Access The ability to access the network and data any time through any device	High	This may imply a truly ubiquitous network. The tower density to realize this goal will exceed current commercial networks.	Cost effective network extension technologies, such as rapidly deployable infrastructure and vehicular network extension products	Backhaul costs and technology limitations will become a significant hurdle	The commercial eco-system continues to innovate on pico and nano cell technologies

Open Standards and Commonality

In virtually every industry we participate in as consumers, open standards are at the core of the industry's ability to create market scale, encourage innovation and create competitive supply chains. The PSWBN, built on open LTE standards is poised to reap similar benefits, at least initially in the Transport Network that is the focus area of these standards.

At a high level, we can view a wireless broadband implementation to include three layers: The Transport Network, a collection of Network Services and a number of mission-specific Applications, as depicted below.



Standardizing on LTE for the Transport Network is a significant first step. Additionally, standardized Network Services such as Short Message Services (SMS) and IP-Multimedia Services (IMS) that are compatible with LTE will provide a foundation for a subset of applications that meet some public safety user needs.

The challenge that will present itself is Network Services and Applications that are unique to the public safety mission, for which open standards to not exist today. For example, mission-critical voice is high on that list, as is situational awareness that includes fusion of voice, video and data content. Content Based Networking (CBN) is emerging as an important paradigm for enabling applications to access content without regard to its network location. Content Based Edge Mobile Networking (CBMEN) takes this to the next level in an environment that requires mobility.

There is often confusion between the demarcation of Network Services and Applications, so to that end, it is useful to consider some examples. Applications that support e-mail are pervasive, running on different operating systems and imbedded within many application suites – yet with full interoperability between these various applications. What makes this possible is the collection of e-mail standards that define the corresponding network services, initially beginning with the Simple Mail Transfer Protocol (SMTP). The World Wide Web is another – Browsers running on many different platforms are fully compatible as they implement the Hypertext Markup Language (HTML) delivered over the Hypertext Transfer Protocol (HTTP).

As NIST contemplates a comprehensive R&D program, Harris recommends that effort be devoted to understanding Applications and Network Services that are unique to public

safety and fosters innovation that can lead to open standards, first within the domain of Network Services, and beyond that, to the degree appropriate, in the Applications themselves.

Multi-Vendor Environments

NIST R&D initiatives should address technical issues that will foster a multi-sourced competitive vendor environment, in which there are, interchangeable building blocks. Multi-Sourcing and Interchangeability are principle means to achieving interoperability. These notions are well aligned with NIST's mission, "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life".[5]

For over eighty years, Harris has brought advanced technologies to public safety, homeland security, national defense, and other mission critical markets. Through these efforts, Harris has learned how leveraging continual technology innovation can have a profound impact on our nation's ability to procure and deploy state-of-the art products and services for these mission-critical markets. Harris has seen that a robust supply chain fostered by appropriate business models and multi-source procurement practices must be implemented to ensure that all levels of government will procure these capabilities in a cost-effective manner.

In order for such a multi-source environment to be fostered, we must focus NIST's R&D efforts in the context of what interoperability means as a threshold matter from the perspective of standards development, governance, and procurement. For the PSWBN to function in the most effective way for first responders and those they serve, interoperability must be viewed as interchangeability: the ability of public safety to interact with a multi-sourced supply chain, grounded in open standards. All critical applications, devices and network technologies should be capable of being used together regardless of brand or network location, and public safety must be encouraged to develop a competitive supply. This definition will allow every first responder to communicate across the nation and will drive suppliers to produce highly innovative and cost-effective products that public safety agencies can procure and deploy with confidence that they will plug and play.

A significant first step in bringing to the PSBWN space a multi-sourced, interchangeable network and device ecosystem was achieved when stakeholders embraced LTE as the standard for the PSWBN. Leveraging this commercial standard will empower manufacturers to begin to address the needs of first responders by evaluating a pool functionalities made possible through open standards. This opportunity is critical: the requirement that the core set of functions of the PSWBN be built upon open standards will enable interchangeability and multi-sourcing.

This leads to another critical element of the PSWBN that has yet to be developed and which NIST is well positioned to craft with its R&D funding and mission. It is vital that a baseline of interoperability capabilities that all manufacturers can and must enable with

---

[5] http://www.nist.gov/public_affairs/general_information.cfm

any product used in the PSWBN be established. This PSWBN Network Profile, described earlier, must be based upon a set of open standards that specifically meet the core needs of first responders in the context of broadband communication. NIST should participate in development of the PSWBN Network Profile and promote open standards that allow for innovation, without hindering interoperability.

To begin assessing what the PSWBN Network Profile should be, we should first examine public safety requirements, the LTE standard, and what parts of that standard fit commercial and public safety needs, respectively. The Venn diagram in Figure 1 articulates the unique standards landscape for public safety. LTE is a sweeping set of standards that exceeds most commercial needs. Thus, commercial manufacturers only utilize a subset of LTE standards. Nonetheless, the core interoperability needs of commercial LTE networks are met through use of these common open standards. To ensure the seamless interoperability, high level of innovation, and cost-effectiveness of the commercial network in the PSWBN space, open standards must envelop the needs of the public safety community.

A three-pronged initiative is needed: First, the public safety community must create the PSWBN Network Profile and identify capabilities not defined in the LTE standards. Next, NIST and manufacturers should collaborate to create open standards through appropriate Standards Development Organizations (SDO's) that bridge the gap between those of LTE and those still needed for public safety. With this full set of open standards, public safety will finally benefit from the commercial network model that makes networks affordable and effective. Finally, there is the need to implement a rigorous IOT process to verify compatibility of multiple vendor solutions.

This is not to say that open standards and the multi-sourced environment will limit innovation or discourage manufacturers to make products with features that enhance an Network Profile. In fact, with open standards that meet the PSWBN Network Profile, manufacturers will be driven to develop products that exceed the profile elements. Though we often buy commercial devices with superior applications or choose a carrier with services that best meet our specific need, we know that the basic interoperability that the open LTE standards afford will serve us when communicating with someone on another carrier or device. This model will encourage this very innovation and sensitivity to meeting the needs of the public safety consumer. Thus, by driving the creation of a PSWBN Network Profile and open standards that meet it, NIST will accelerate innovation, multi-sourcing, product interchangeability, and true interoperability.

Affordability

Harris believes that central to the issue of affordability is the business model embraced for the design, construction, operations and maintenance of the PSWBN. Key tenants of that business model that can drive affordability are:

1. Leveraging commercial eco-systems
2. Emulating commercial network operator business models built on the principles of multi-sourcing
3. Directed Research & Development that gets to the heart of the cost drivers for public safety equipment and services

The very essence of a commercial network operator's business model is to ensure financial success. The benefits of items 1 and 2 above have been discussed earlier. Here we want to introduce one more driving factor – Purchasing Scale.

It is well understood that economies of scale drives cost and hence contributes significantly to affordability. Historical practice in the public safety community is procurement on a jurisdictional basis. Inherently with this practice, many economies of scale cannot be achieved. Indeed, without scale, multi-sourcing may not be a viable procurement strategy. While the PSWN will not achieve the scale of commercial networks in terms of users, infrastructure deployment will very much parallel the scale of commercial networks.

One potential difference to note is that site/tower density in commercial networks is often related to capacity needs and not to coverage. It is reasonable to expect that there will be many public safety situations where site/tower density is related to coverage and not to capacity. So, on the whole, site/tower densities for the PSWBN will rival those of the nationwide operators, albeit with a potentially different distribution of locations.

Another key on network affordability is in end user devices. Part of the goal of leveraging commercial technologies in the development of the PSWBN is to obtain some of the economy of scale of the commercial device ecosystem. Unfortunately, the ecosystem may not support some of the key public safety features. Part of the R&D effort from NIST can focus on helping drive the key public safety features into this device ecosystem – or to find a way to leverage the commercial ecosystem and add these features at low incremental cost.

Survivable Core & Cyber Infrastructure

Cyber crime and cyber terrorism will be one of the biggest threats to our society and welfare. In that light, it is appropriate for our nation to address this threat, for both the commercial infrastructure that we rely on as consumers, and for purpose-built networks such as the PSWBN. It has been pointed out earlier that while building the PSWBN on LTE standards brings many benefits, it also brings with it inherent risk that current public safety systems do not have. Today's jurisdictional Land Mobile Radio (LMR) networks are largely isolated from one another, such that failure in one system does not propagate to other systems (of course this is also part of the challenge achieving interoperability between these disparate systems).

Implementation of a core network that serves the entire PSWBN will be a key enabler of nation-wide interoperability. Such a core must be implemented in a distributed architecture that ensures network resiliency, reliability, and availability are not compromised. The opportunity to leverage a survivable core built on cyber-infrastructure is significant and should be investigated. To that end, it is appropriate to decompose the PSWBN transport network into three logical components:

The PSWBN LTE Core Network will be built in accordance with LTE standards, and is known as an Evolved Packet Core or EPC. Current Part 90 rules articulate the specific EPC interfaces and logical functions that are required to be implemented in the PSWBN LTE Core Network.

The PSWBN LTE Radio Access Network (RAN) will also be built in accordance with LTE standards, and is known as the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Current Part 90 rules also articulate the specific interfaces that are required to be implemented in the PSWBN RAN.

LTE is a flat Internet Protocol (IP) based network architecture. Interconnection of the EPC and RAN components is over IP network connections. The large number of these interconnections collectively forms the Backhaul Network.

Implementation of the Backhaul Network is highly synergistic with the notion of a survivable core built to robust cyber-security requirements. The PSWBN LTE Core Network can be viewed as being layered on top of this survivable IP core network that forms the backhaul for interconnecting the PSWBN LTE Core Network components and

the PSWBN LTE Radio Access Network (RAN). Harris recommends that NIST consider R&D efforts to assess viability of this concept.

Industry Engagement

Harris applauds the on-going dialog that the Department of Commerce has fostered with public safety practitioners and industry stakeholders. Organizations such as NIST and VCAT together with initiatives such as the Public Safety Communications Research Program (PSCR) have enabled interchange of ideas on multiple levels. This solicitation is further progress on expanding that dialog in the context of Research and Development initiatives that the Department of Commerce can fund and provide oversight for.

The public safety industry is not a monolithic market. It is comprised of numerous state, local, and tribal organizations, in collaboration with a number of Federal agencies. Industry groups such as NPSTC and APCO have played a key role over many years to foster development and advancement of the state of the art for public safety communications. The FCC, with its regulatory oversight charter has an expanded role via the Emergency Response Interoperability Center (ERIC). Standards Development Organizations (SDO's) such as 3GPP, ATIS, TIA, and IEEE will play ever-more important roles as the emphasis on open standards increases. At the intersection of standards and technology, NIST has a particularly relevant role to play in shaping the future PSWBN. Public safety is also supported by a vast eco-system of technology, product and solution providers. Finally, commercial operators bring a wealth of relevant experience to the table. Harris recommends that NIST foster venues that bring these stakeholders together.

CONCLUSION

Public safety is poised to leverage evolving 4G wireless broadband technologies in ways that will enhance their ability to perform their mission. Availability of a dedicated block of nation-wide spectrum and comprehensive commercial standards are two foundational elements that form the starting point. NIST properly recognizes that there are gaps between requirements articulated by public safety and capabilities defined by these commercial standards and associated products available from commercial OEM's. The R&D program that NIST envisions can be a significant step towards closure of those gaps. To that end, Harris is pleased to provide input to NIST on these issues of great national importance.

Respectfully submitted,

Dennis Martinez
Chief Technology Officer
Harris RF Communications Division

October 12, 2011