Introduction

This document is in response to the NIST document "**RFC Nationwide Public Safety Broadband Network**" Docket No.: 110727437-1433-01. Following are responses from xG Technology, Inc. concerning the requested comments in the noted RFC. Some responses are left blank as a specific best practice or industry gap was not cited for this parameter.

We begin below with an introduction to xG's, xMax product. Following that, you will find our responses to the Feature List questions, then Table 1 and our responses to the network questions. Finally, Table 2 and our responses to the more general questions posed in the RFC.

Contacts

Please forward any questions or return comments to Michael Johnson (Michael.Johnson@xgtechnology.com) or Kevin Zern (kevinz@xgtechnology.com)

xMax

xG Technology has been developing xMax, an end-to-end all-IP cognitive radio access network (C-RAN) to support low-cost, carrier-grade mobile voice and data services on licensed and unlicensed spectrum. Currently, xMax offers mobile communications on a software-defined radio (SDR) technology framework that includes frequency agility, interference-mitigation and avoidance algorithms, and mature commercial off the shelf (COTS)/Internet Protocol(IP) building blocks (such as session initiation protocol (SIP) and real-time transport protocol (RTP)). xG's original intention for xMax development was entirely focused on commercial markets. That being said, the cognitive properties and the capacity of xMax to deliver dynamic spectrum access (DSA) make it an attractive, scalable cellular platform worthy of consideration for employment by the Public Safety community.

It offers the following key benefits:

- **Self-Frequency Planning** - the system comes up automatically and finds available frequencies, no manual frequency co-ordination required

- **Self-Optimizing**- the system uses Dynamic Spectrum Access technology to maximize throughput and reliability, delivering a licensed spectrum experience in unlicensed spectrum

- **Leverages existing smartphones, laptops, tables, etc**. directly into the xMax mobile radio network to save costs and offer unmatched applications and functionality

- **End-To-End IP Architecture** - .simplifies integration with LTE, P25 and other networks via industry standard interfaces and protocols

- **Tactical and Scalable Deployments** – rapidly deployable size and weight, proven integration with satellite and point to point backhaul radios

- **Difficult to Jam or Hack** – Dynamic channel/band hoping makes attacks and penetrations far more difficult than traditional radio systems

In particular, the spectrum agnostic and interference mitigation operating parameters of xMax support a level of radio interference tolerance previously not seen. The implications of these operating parameters are significant and provide for the enhancement of communications and successful First Responder and Public Safety missions, while not creating additional spectrum management challenges or risk running afoul of other commercial wireless systems. Further, the DSA capability and concomitant ability to employ unlicensed spectrum offers potential to dramatically reduce system operating cost when compared with commercially available cellular alternatives. Finally, xMax is capable of providing a cognitive cellular capability that could opportunistically 'roam' on other commercial cellular network infrastructure if needed.

In short, xMax has the potential to close a critical communications capability gap and provide Public Safety with an affordable, independent, enterprise handheld wireless service. xMax is

fully expeditionary and provides a level of resilience and continuity of operations that safeguards *mission-assured* communications, regardless of circumstance.

The xMax network is designed to utilize unlicensed spectrum in a cognitive manner. The goal of the network is to make unlicensed spectrum perform as well as licensed spectrum. The network system accomplishes this using cognitive technology. All devices are frequency agile and use "edge" driven decisions to find available spectrum and avoid interference. Because of its spectrum agnostic attribute, xMax can be deployed to embrace and employ the 10MHz of spectrum (770-775, 800-805 MHz) that the FCC has already established for public safety in addition to the 126MHz of unlicensed spectrum it is currently being developed for (902-928 AND 5.8X-5.9X).

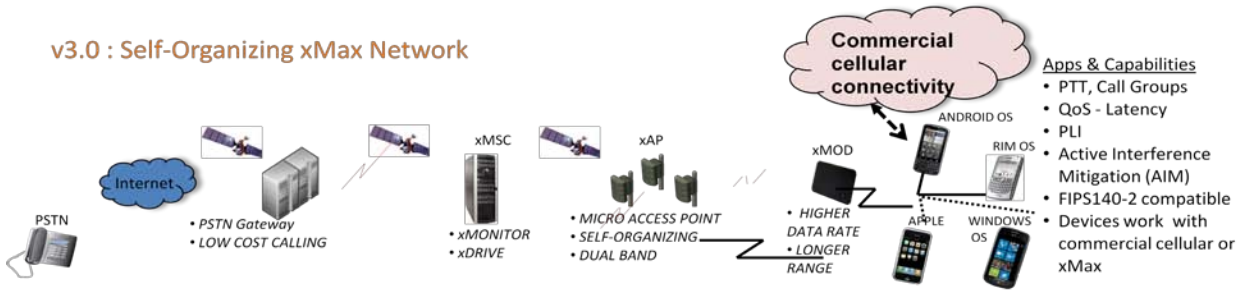
Adaptive modulation and robust multiple input multiple output (MIMO) physical layer (Radio PHY) allow the network to operate in the presence of interference. A very capable signal processing system allows the network to perform passive beam forming and intelligent error correction to mitigate persistent interferers. Three devices compose the network.

The xMax modem (xMod) is a mobile personal "hotspot" device that bridges 802.11 devices to the xMax network. It is portable and battery powered. It looks like an 802.11Access Point (AP) to devices like smartphones and laptops. It looks like a subscriber device to the xMax network. The xMod is a very capable receiving device that supports 2x4 MIMO and OFDM PHY.

The second device is the xMax Access Point (xAP). This device has multiple channel units, is approximately 16"x10"x6", and light enough to be pole or vehicle mounted. This device provides the xMax PHY to standard IP protocol conversion. It manages xMods and channels.

A third logical device is the xMax Mobile Switching Center (xMSC). This is a set of COTS servers and firewalls with xG developed configuration. This configuration uses xG patented compression algorithms to improve SIP signaling and over the air RTP for VOIP and video.

The network is IP from end to end and supports any application developed for laptops or smartphones that have a WiFi interface.



FEATURE LIST
Resiliency: The ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements.
➢ Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network--- Very Important
➢ How our team's offering currently meets this feature: *xMax system is designed to be transportable, initialize quickly and adapt to the local environment. It employs Dynamic Spectrum Access (DSA) to find and automatically employ spectrum. DSA also allows the network to avoid interference. Beyond DSA, xMax applies interference processing to mitigate interference to provide broadband service in crowded (dirty) spectrum.*
➢ Current gaps that exist preventing the realization of the full potential of the feature: *Most networks use a fixed frequency allocation with static channel assignment. Restoration of services under these constraints conveys significant delays due to the imperative to remap the established frequency plan onto the contingency response network. Frequency agnostic networks employing cognitive technology and DSA avoid this conflict. The xMax system combines environmental sensing algorithms fed by advanced Orthogonal Frequency Division Multiplexing (OFDM) and Multiple Input Multiple Output (MIMO) processing to deliver services in heavily challenged environments too difficult for 3G and 4G LTE systems.*
➢ Possible research and development that could take place to close any technical gaps: *The most resilient networks will feature secure, interference-resistant, self-forming, self-healing nodal and peer-to-peer exchanges, combined with enhanced capabilities to close link margins in heavily stressed environments. xMax 4.0 intends to incorporate these MANET and security properties given the necessary research and support.*
➢ Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions: *The most immediate challenge will be the commitment to sustain the existing infrastructure and a contingency cognitive/DSA capability simultaneously. Over time, the antiquated infrastructure could be replaced with the advanced operating properties and parameters to ensure both resiliency and accelerated restoration properties. Public safety network equipment requires frequency coordination, deployment planning, and conditioned shelters.*
➢ Best practices from other industries that could be leveraged to expedite public safety's realization of these key features. *Build underlying networks that support newer interoperable protocols in critical areas. Use unlicensed spectrum + licensed spectrum to meet network goals.*
Self-Organizing: Self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.
➢ Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important

- How our team's offering currently meets this feature:

  The xMax network is self organizing, employs DSA and requires no channel planning. The AP devices initialize and scan to assess the environment, then select channels for operations and signaling. The subscriber devices listen to this signaling and determine the "best" channel for operation. They associate with an AP type device, but keep background scanning to determine a better channel. The xMax network also manages data rates, antenna beam forming, and transmit power levels, all in response to dynamically changing network conditions.

- Current gaps that exist preventing the realization of the full potential of the feature:

  Existing and identified growth systems such as 4G LTE rely upon clean, reserved spectrum for operation. Establishment of MANET capability within this framework and deployed protocols will require significant alteration of the existing and planned software models. The xMax system is designed to incorporate MANET within its technology development roadmap.

- Possible research and development that could take place to close any technical gaps:

  Given the resources and sponsorship, xG Technology, Inc., is prepared to develop and deliver a defined area MANET network within 15 months of commencement.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

  Delivering a MANET network is a holistic process. The strength and resiliency of the network rides on the diversity and redundancy of the interconnected nodes. At least one node must be connected line-of-site (LOS) to the Access Point, and the most isolated operator must have at least one other unit within LOS. The challenge is to embrace the network as a system and provide the resources to field a full-scale pilot program to validate the efficacy of moving forward from traditional hub and spoke architecture.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

Meshing (ad-hoc device-to-device communication): A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important

- How our team's offering currently meets this feature:

  The xMax system uses a TDMA Media Access Control protocol. This TDMA frame is designed to support Meshing. Each node can become a relay node. This will allow each unit to hop through other units to find a destination or access a connection to another network. The units will utilize an on demand routing protocol that will allow discovery of other nodes with low overhead. Development of this mobile ad hoc networking (MANET) schemata will deliver full network services to the most isolated operator. Snipers and overwatch personnel will share the situational awareness (SA) of the

assault team. Negotiators will have cognizance over the real-time operational deployment. The Special Forces community has mastered the shared SA operational tactic. xG brings in the expert team to implement the full mesh network to its ultimate advantage.

- Current gaps that exist preventing the realization of the full potential of the feature:

  Ad hoc mesh networking architecture requires an investment in an end-to-end system. xG Technology is well advanced in formulating the algorithms and physical footprint to deliver full MANET capability to the First Responder Community. NO PHYSICAL IMPAIRMENT PRECLUDES DEVELOPMENT; full system delivery will be paced by commitment of resources, and commitment to deliver. xG is committed to delivering full system capability at an affordable and sustainable rate.

  Equipment designs that support the functionality needed for a Mesh system. Handheld devices capable of Mesh operation. Adoption of ad hoc routing protocols.

- Possible research and development that could take place to close any technical gaps:

  xG is pursuing the building blocks for MANET networks in its initial commercial offering. Advancement to a full mesh network is a straight forward path, and one that can be built in increments to ensure value and ROI at every step along the way.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

  The pacing item for full capability will be the commitment to an enterprise architecture and infrastructure. The voice-centric hub-and-spoke structure of the legacy systems, and the 3G/4G LTE horizon proposals lack the capacity to self-form and self-heal. The first and greatest hurdle will be implementation of a robust pilot program to validate the advantages and affordability of mesh networking. xG's partnership approach greatly lessens the investment and risk over traditional service providers.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

  Employ the Southwest Airlines model of equipment commonality to minimize total ownership costs. SWA has the highest cockpit cost and the lowest total flight hour cost of all the major carriers. The SWA model demonstrates the power of minimizing logistics expenses. The First Provider edge services arena, the imperative is to move away from single-vendor, limited utility end items, to ubiquitous smart devices which can be replaced for nominal cost to keep pace with technology and services advances.

  Buy or lease equipment that is software upgradeable so its functionality can be upgraded without replacing hardware.

Adaptability: The ability of the network and/or device to modify/change behavior based upon external conditions.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network-Very Important
- How our team's offering currently meets this feature:

xMax utilizes a web configurable rules table. This allows the system to use or dis-allow any spectrum block or slice. The rules allow the system to dynamically size or release spectrum for instant backup of legacy systems should those legacy systems fail or go dark. This is similar to the way UPS systems provide backup power when power mains fail. xMax could be utilized in much the same way to automatically provide backup communications when the main systems fail. Simple operational rules make the system extremely flexible.

- Current gaps that exist preventing the realization of the full potential of the feature:

  Software defined radios (SDR) have not been utilized in public safety applications.

- Possible research and development that could take place to close any technical gaps:

  SDR is a proven commodity widely employed around the world, including the combat zones in Iraq and Afghanistan. Yet to be developed is a more robust security system for the physical address layer of the nodes/operators in an SDR-enabled network. Accreditation and certification of the integrity of this layer should be part of overall system development.

  A study of real time utilization of public safety frequencies in support of using SDR.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions?

  Public safety legacy gear is based on fixed function devices that cannot take advantage of SDR type capability.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

To ensure reliability and availability:

Prioritization: The ability to prioritize network traffic based on assigned priority schemes.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important

- How our team's offering currently meets this feature.

  The xMax system is an all IP network. Using local DSCP settings a user or application data can be prioritized for transmission. The ability to prioritize single users (i.e. the Fire Chiefs unit) can be accomplished using local priority settings. Multiple levels of priority are assignable to end user devices.

- Current gaps that exist preventing the realization of the full potential of the feature:

  The ability to automatically recognize prioritized data from node to node is not well developed. This would be like deep packet inspection at every node, but the inspection would be to who or what group the data was going to as well as what data type it was.

- Possible research and development that could take place to close any technical gaps:

  Research could be done on selectively prioritizing individual groups or users for voice and data.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

  Public safety networks have the concept of individual priority (like when a Police Chief gets priority). They don't have the concept of classifying users/data to finer degrees.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

Quality of Service (QoS): The set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over provisioning their networks. The goal of QoS is to provide preferential delivery service for the applications that need it by ensuring sufficient bandwidth, controlling latency and jitter, and reducing data loss.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important
- How our team's offering currently meets this feature:

  The xMax system supports current QoS protocols like 802.1p. A TDMA MAC is employed to give very deterministic packet transmission times. Packets like voice and video that are time sensitive are prioritized over less time sensitive data at every level of the xMax system.

- Current gaps that exist preventing the realization of the full potential of the feature:

  Data services that support system wide recognition and processing of QoS for packet types and individuals are not widely deployed in Public Safety systems.

- Possible research and development that could take place to close any technical gap:

  The feasibility for deep packet inspection for data type and user priority at all nodes in a public safety network.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:
- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

To enable security:

Strong, Dynamic Access Control: Access control lists can be configured to control both inbound and outbound traffic on networks and authentication/verification of users/devices on the network.[7] The level of access control should be sufficient to allow for entrée into a broad set of systems and databases needed by public safety (e.g., criminal history databases, medical records, public work records, etc.).

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important
- How our team's offering currently meets this feature:

  The xMax network employs AAA functionality to authorize and authenticate network users and infrastructure.

- Current gaps that exist preventing the realization of the full potential of the feature:

  Current public safety systems use different authentication schemes. Bringing together disparate groups and dynamically adjusting the authentication process is not well developed at this time.

- Possible research and development that could take place to close any technical gaps:

  Many research papers have been written on the subject. Practical procedures for deploying a mixed organization authentication system would be a good topic for discussion.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

  Public safety has a vendor centric view of security. The networks don't interoperate well.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

To ensure affordability/commercial alignment:

Compatibility with Commercial Infrastructure: The utilization of a variety of commercial services when public safety is in areas not covered by the public safety broadband network.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important

- How our team's offering currently meets this feature:

  One of the components of the xMax system is the xMod. The xMod connects WiFi devices to the xMax network. All of the laptops and smart phones currently in use by the public safety agencies that are equipped with WiFi will be able to work with the xMax network unmodified. Different agencies can use the xMax network as long as the devices support WiFi. Since the system is all IP and uses existing smartphones and laptops as subscriber devices, many off the shelf applications like push to talk and position location are already available.

- Current gaps that exist preventing the realization of the full potential of the feature:

  The creation and adoption of devices that support P25, military and Cellular protocols are nonexistent.

- Possible research and development that could take place to close any technical gaps:

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

  Drive the public safety and cellular industry to provide what is needed for high function mission critical networks.

Network sharing: The shared use of infrastructure between commercial and public safety users.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important

- How our team's offering currently meets this feature:

  One of the components of the xMax system is the xMod. The xMod is a portable or mobile installed device that connects to the xMax wireless network, and then forms a WiFi hotspot in and around the mobile or remote location for access by any and all COTS WiFi enabled devices. All of the laptops and smart phones currently in use by the public safety agencies that are equipped with WiFi will be able to work with the xMax network unmodified. Different agencies can use the xMax network as long as the devices support WiFi. Since the system is all IP and uses existing smartphones and laptops as subscriber devices, many off the shelf applications like push to talk and position location are already available. One set of xMax infrastructure could be installed and smart devices from many agencies could use this network as a shared resource.

- Current gaps that exist preventing the realization of the full potential of the feature:

  Bridges are not readily available that allow cellular and public safety devices to share the same network.

- Possible research and development that could take place to close any technical gaps:

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

Multi-Modal: The ability of the network to support voice, video, data, and multimedia simultaneously.

- Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important

- How our team's offering currently meets this feature-

  The xMax system is designed to support voice, video and data simultaneously on the same network. The network is an all IP design. Priority for latency sensitive data is built into the system. All payloads are data in the xMax system.

- Current gaps that exist preventing the realization of the full potential of the feature?

  Most public safety handheld units are not designed for Multi-Modal payloads. Also spectrum available is limited, so only low bandwidth applications are employed.

- Possible research and development that could take place to close any technical gaps:

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

Scalability: The ability of a system, network, or process to handle growing amounts of work in a graceful manner or its ability to be enlarged to accommodate that growth.[8] At the design

phase, this could include requirements to ensure that scalability can be achieved, to the extent possible, by software enhancements and upgrades as opposed to by hardware replacements. Scalability also includes the need, in the case of a large scale event, to accommodate a rapid increase in the number of users in a limited geographic area.
➢ Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important
➢ How our team's offering currently meets this feature- *The xMax system has no system limitations on the numbers of users or addresses that can be allocated. The system is self organizing and self healing. With over 135 MHz of spectrum available to xMax, few limitations inhibit growth of the network to meet traffic needs.*
➢ Current gaps that exist preventing the realization of the full potential of the feature: *Current systems use fixed amounts of spectrum and rigid function devices. This limits the capability to dynamically scale.*
➢ Possible research and development that could take place to close any technical gaps: *The usage of cognitive network equipment to increase scalability.*
➢ Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:
➢ Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:
Power Awareness: The ability of network/devices to control power functions.
➢ Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Important
➢ How our team's offering currently meets this feature: *The xMax network components can change output power based on network situational awareness. Power is reduced and increased for optimum transmission of data, minimal self interference in changing network conditions and increased battery life.*
➢ Current gaps that exist preventing the realization of the full potential of the feature:
➢ Possible research and development that could take place to close any technical gaps:
➢ Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:
➢ Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:
Standardized Common Interfaces: Protocols, Application Program Interfaces, application platforms, radio capabilities, etc. that allow for competitive provisioning.
➢ Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network- Very Important
➢ How our team's offering currently meets this feature: *The xMax system is based on many standard interfaces and protocols. The network supports IP communications. WiFi is a supported access protocol. Ethernet and Fiber*

are defined network interfaces. SIP signaling is employed. The network is all IP.
➢ Current gaps that exist preventing the realization of the full potential of the feature: *Many public safety networks today use proprietary vendor protocols between components.*
➢ Possible research and development that could take place to close any technical gaps:
➢ Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions: *Most public safety equipment does not support open protocols at air link and infrastructure levels today.*
➢ Best practices from other industries that could be leveraged to expedite public safety's realization of these key features: *Pick a set of standards and leverage them across public safety agencies. Enforce buying based on standards support.*
Uniform, Universal Access: The ability to access the network and data anywhere at any time through any device.
➢ Our team's assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network -Very Important
➢ How our team's offering currently meets this feature: *The xMax network was designed to allow off the shelf smartphones, tablets and laptops to be used without modification. This is based on a common WiFi interface. All of these devices can access the network anytime. The xMax network operates in unlicensed bands so can be set up anywhere in North America. What does not exist today is a gateway from legacy P.25 or analog narrowband devices to gate them to an IP network.*
➢ Current gaps that exist preventing the realization of the full potential of the feature Public safety, military and cellular systems don't gateway or interact today:
➢ Possible research and development that could take place to close any technical gaps:
➢ Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:
➢ Best practices from other industries that could be leveraged to expedite public safety's realization of these key features:

Table 1 Network Questions

What is the importance of employing open standards for the nationwide public safety network?	Open standards allow for networks to more easily interoperate. Devices and infrastructure can take advantage of economy of scale and reduce costs. More integration of standard components will likely increase battery life.

What is the need, if any, for commonality of functions across the system?	Common functions reduce user training and allow the vendors to build a common device that supports this set of functionality. During disasters new or shared equipment can be more easily used by disparate groups because it functions the same.
What is the importance of a multivendor environment for the network and what are the lessons learned in deploying a multi-vendor environment from the cellular and other industries?	Multivendor environments can lower cost and increase supply of equipment. Lessons learned from cellular are that a consistent set of standards must be used to enable a multivendor system to operate.
What can be done to ensure both short- and long-term affordability of the network for all types of public safety agencies?	Create public safety networks that can use mass produced devices. Develop protocol converters that allow legacy systems to communicate with new networks.
In a recent report, the President's Council of Advisors on Science and Technology suggested the need to develop methods for implementing a ''survivable core'' of cyber-infrastructure that would be relied upon to provide truly essential services in the event of a catastrophic cyber-attack.9 Please comment on how NIST should pursue this recommendation. Among other things, commenters should address whether the goal should be to design a separate survivable core that is integrated and interoperable with the primary public safety network, or instead to design the primary network such that it can reconstitute rapidly— following a catastrophic event— to achieve some ''core'' level of service.	A technology core that is isolated and can be quickly reloaded would seem to be the best solution. Have duplicate offline equipment that is sufficient for a core set of functionality. Have it also loaded with validated software versions. In the event of cyber-attack, isolate network connections, and bring up the core set of equipment. Use tools on the core set to salvage situational data bases or other information.
What is the marginal cost of the feature/functionality versus equipment available today?	This question was unclear to us. The cost of what vs. what?
What network features or requirements have not been identified above, the lack of which may impair the network's ability to adequately serve the needs of public safety?	Using cognitive capabilities to employ multiple bands of licensed and unlicensed frequencies that can be put into service during a disaster or overloading of the normal network.
How should NIST engage public safety practitioners and technologists as part of the planned R&D projects to ensure proper prioritization of efforts and effectiveness of developed solutions?	NIST should work with vendors and institutions to fund research and development needed to advance the issues listed in the previous sections.

Table 2 General Questions

(1) A dedicated high-quality network connection always available for sending and receiving continual data streams to support monitoring and resource tracking;	xMax is a dedicated mobile network designed to support voice, video and data streams from laptops or smart phones.
(2) At a minimum, access to initial and updated basic incident information (voice- and text-based incident data);	xMax supports mobile access to IP networks from laptops or smartphones.
(3) An infrastructure that is hardened and secure, providing a high level of system availability;	The network is highly available. Hardening and FIPs type certification need to be developed. Network elements are frequency agile and work together to overcome loss of infrastructure or local interference
(4) When voice is converged for normal operations and in the event the infrastructure is compromised, public safety communications must remain stable and with clear voice communications;	Voice is another data application for xMax. VOIP packets are given highest priority in the network.
• Infrastructure-less communications, with talk-around for the ability to talk one-to-one and one-to-many	PTT applications exist for IP networks like LifeRing or Teamspeak. These applications provide 1 to 1 or 1 to many.
• Optimal audio quality during adverse field conditions	Voice is given highest priority.
• No latency on mission critical voice applications	
(5) Geographic coverage that has no limitations within the footprint of the National Public Safety Broadband Network;	The network can be constructed anywhere that allows unlicensed band operation.
(6) Dynamic management and control of the network;	Network supplies xMonitor software package to gather statistics and monitor network elements. Elements are dynamic and act on their own to find and use the best spectrum.
(7) Interoperability, including with existing public safety-based systems;	xMax interoperates with devices like laptops and smartphones. No specific P25 or narrowband analog gateway has been developed.
(8) Ability to send and receive large amounts of information;	Network is all IP and able send and receive large amounts of information
(9) A non-proprietary network based on industry standards;	xMax network is built using all IP network. WiFi is an interface standard. Ethernet is an interface. The network supports VoIP, video,

	web browsing, data base access, YouTube, Facebook...etc.
(10) Single devices that support voice, video, and data;	Network uses devices that exist already. Smartphones and laptops.
(11) Access to and from external information sources;	Yes—IP connection to the Internet.
(12) Easy integration with other technologies;	Yes—load applications on smartphones or laptops and use the xMax network to access open or closed IP network services.
(13) Automatic management and control of the network;	xMax provides xMonitor software to manage and monitor devices.
(14) Current and future enhancements available to commercial consumers are provided to public safety with no limitations; and	Point of this question is unclear. Network enhancements are available to all devices operating on the network.
(15) Ability to send, receive, and process information from the public (citizens and media).	Devices on xMax system can access external websites and data bases and applications as long as the IP network is configured for external access.