Before the
DEPARTMENT OF ENERGY
Washington, DC 20585

In the Matter of:	)
	)
Implementing the National Broadband	)
Plan by Studying the Communications	)
Requirements of Electric Utilities To	)
Inform Federal Smart Grid Policy	)

COMMENTS OF MOTOROLA, INC.

Motorola, Inc. ("Motorola") hereby responds to the National Broadband Plan Request for Information (" NBP RFI") on the communications requirements of utilities, including but not limited to requirements for Smart Grid.[1] Motorola supports the efforts of the Department of Energy ("DOE") to fully assess utilities' requirements before the communications solutions for Smart Grid and other requirements are addressed. Based on Motorola's experience in providing communications systems for utilities, public safety, enterprise, and business users, as well as for commercial carriers and the general public, it is clear that there is no substitute for understanding the user needs first and then applying viable technology solutions to meet those needs.

As addressed herein, examination of the requirements shows there are elements of utility communications that can be served by a commercial carrier, but many other elements require a more secure, highly reliable communications system under the direct control of utilities. Also, separating the generation and distribution elements from the "consumer-facing" functions in the overall Smart Grid network provides increased security from cyber and terrorists attacks of our electric grid, a key requirement for homeland security.

---

[1] Request for Information (RFI), Federal Register, Vol. 75, No. 90. May 11, 2010 at pages 26206-26208.

I. Introduction and Key Policy Recommendations

In its NBP RFI, the DOE asks a number of very pertinent questions concerning utilities communications requirements. It is also clear from the NBP RFI that DOE is aware of information already submitted on this issue in other venues. For example, the NBP RFI references comments previously submitted to the Federal Communications Commission:

> While it appears from comments filed with the FCC that many commenting utilities want to use private, noncommercial networking options, some utilities have also commented that dedicated utility spectrum may be beneficial, but perhaps not essential to continue current Smart Grid deployments like backhaul for meters in an AMI system. One commenter expressed the need for greater industry collaboration to build a better case for dedicated spectrum. Utilities have also expressed a need for dedicated spectrum for fast power restoration in an emergency or natural disaster, reliable service, and for protection from a cyber attack on the electric grid. DOE thus seeks to better understand this need for dedicated spectrum; what compels the need for additional spectrum in addition to the increased amount of data that utilities are expected to handle as the deployment of Smart Grid applications multiplies.[2]

Motorola believes the information provided herein, together with information from utilities who are on the front line of the Smart Grid requirements, will provide DOE with significant guidance to address spectrum issues. As addressed more fully in these comments, Motorola believes that some elements of the Smart Grid communications can be addressed on commercial systems, but that many other communications for Smart Grid as well as utilities' other communications requirements, require dedicated spectrum.

Unfortunately, utilities and other businesses that rely on internal communications systems, have not been granted additional spectrum since Congress authorized the use of auctions to license commercial spectrum bands. Motorola recommends that DOE focus closely on utilities' actual operating requirements in addressing policy issues on communications solutions. Meeting these requirements is urgent as a potential cyber or terrorist attacks on our

[2] DOE NBP RFI Federal Register Notice at pages 26207 and 26208.

electric grid may be prevented by more secure communications networks under the utilities' direct control. Failure to secure this asset could set off a wave of consequences that significantly impact our country.

Motorola recommends that DOE consider the security benefits that occur by separating the power grid network generation and distribution control functions from "customer-facing" elements of the Smart Grid communications. For example, communications and control for the generation and distribution functions would be deployed on a private network under the control of utilities. Automatic Meter Infrastructure ("AMI") functions that position every residential and industrial electric meter as a possible entry point into the system would be conducted over a commercial network, separated from the private internal system. Doing so can provide an extra element of security that would not exist if all functions were either on a commercial network or on a private system.

These critical communication needs are best served by a private network as opposed to a commercial network with priority access; there is no guarantee that communications over a commercial network would be available in times of emergency. Commercial networks are designed and deployed to serve the average requirements of their consumer customers. Experience shows that during emergencies commercial systems can become unavailable or clogged with consumer communications.

Even public safety users with priority access cannot obtain service, so it is likely utilities would have a similar experience.[3] In an emergency, some utility communications functions are

[3] See Comments of the National Public Safety Telecommunications Council, Docket Nos. PS 06-229, submitted to the FCC July 2, 2010 and *Subject to Debate- A Newsletter of the Police Executive Research Forum,* Vol. 24, No.3, March 2010. Both describe actual experiences in which public safety agencies with priority access failed to obtain communications on a commercial network during emergencies.

as essential as those formally classed as public safety. Motorola believes that there are more similarities between utilities' and public safety's broadband requirements than there are between those of utilities and commercial networks. Therefore, Motorola recommends that DOE take into account the experiences of public safety with commercial networks during emergencies, as that experience is also generally applicable to utilities' communications requirements. For some utilities' communications requirements, it may be beneficial to consider public safety/utility partnerships.[4]

In summary, Motorola's key policy recommendations are as follows:

- Utilities' operational requirements should be the primary foundation for DOE decisions and recommendations to sister Federal agencies.
- Some elements of utilities' communications requirements are compatible with commercial networks; many elements that are more mission critical are not.
- Utilities and public safety have more in common in their critical communications requirements than utilities and commercial wireless operators.
- To the extent utilities and the public safety entities find it beneficial to consider any partnerships, the DOE and FCC should seriously consider a foundation for such partnerships. The primary elements pertinent to such partnerships that Federal policies in DOE and the FCC can influence are the availability of sufficient spectrum with the right provisions for control to meet utilities' and public safety's respective operational needs.

II. Response to Specific Questions in the NBP RFI

The RFI raises a series of specific questions with regard to utility communications. Motorola provides detailed input in response to these questions in the attached appendix.

III. Conclusion

Motorola supports the NBP RFI initiative by the DOE to help determine utilities' communications requirements for Smart Grid, as well as other key functions. Among the many

[4] This may be especially useful for municipal utilities.

factors to consider, Motorola believes utilities' operational requirements are first and foremost and should be given high priority in the complex but necessary analysis to determine how communications requirements should be addressed going forward. Motorola has provided significant details in the attached Appendix in responding to the questions DOE included in the NBP RFI. We believe this information will be a valuable part of the analysis and deliberations on utilities' communications requirements.

Respectfully submitted,

/s/ Robert D. Kubik
Robert D. Kubik, Ph.D.
Director, Telecom Relations Global

July 12, 2010

Appendix – Detailed response to DOE NBP RFI Questions

1. ***What are the current and future communications needs of utilities, including for the deployment of new Smart Grid applications, and how are those needs being met?***

Utilities currently rely on wireless communications, both for internal purposes and for external communications with the public. Reliable internal wireless communications provides a necessary foundation to ensure worker safety, transmit information to/from workers in the field to enable efficient and cost-effective operations, provide fast and efficient power restoration during outages, coordinate priority work with public safety entities during an emergency, support basic monitoring and control (Supervisory Control and Data Acquisition, "SCADA") and meet other local, state and Federal requirements applicable to the utilities. While communications with the general public can be handled over commercial networks, internal communications are typically handled over dedicated, utility controlled systems designed to meet more stringent reliability, availability, coverage and low-latency requirements. Unfortunately, the lack of any additional dedicated spectrum allocations for utilities has hampered expansion of these internal communications systems to meet operational needs.

Increasingly, additional communications are also required for machine-to-machine functions to control and monitor power generation, distribution and usage, i.e., the key elements of a future Smart Grid system. Smart Grid communications has a set of differentiated if not unique needs:

- Performance – Since Smart Grid communications are machine to machine and include real-time control, the bandwidth (bit rate) required is relatively modest but low latency is of extreme importance for some applications.

- Reliability – The need rises to a "mission critical" level as more applications involving distribution control are automated and networked. In the future, the distribution system will require communications be available before electric power can be supplied. Power savings from Smart Grid are expected to reach a significant portion of the cost of building out additional generational assets. When that happens, the benefits of Smart Grid play a key role in a utility's overall resource landscape and reliability. Communications requirements for Smart Grid generation and distribution functions should therefore be categorized as mission critical.

- Coverage – Electric utilities provide services over their entire service area. The Smart Grid communications requirement is also for the entire utility service area. Commercial networks are built to meet the needs of the population they serve and may not provide coverage over the same service area required for utilities' communications, including the Smart Grid. It is important to recognize that covering a certain percentage of the population is significantly different from covering a similar percentage of the geography. For example, on a nationwide basis, a system that covers 95% of the population may

cover only 45% of the geography. Even a 98.5% population coverage translates to only about 63% of the geography.[5]

Smart Grid communications needs can be broken into its component key elements to address requirements and viable solutions. For example, AMI is a somewhat less critical function that tolerates higher latencies and should be accomplishable in metro areas over a commercial network. In addition, cost effectiveness of the solution is a key factor for AMI devices to be deployed on residential meters. Leveraging the economies of scale across both AMI and commercial wireless devices provides these economies of scale. DOE should also consider input from utilities regarding any per unit monthly charges for AMI devices to communicate over a commercial network. Extending AMI to lesser populated areas would require other wireless alternatives if there is no commercial wireless coverage in those areas.

In contrast, other elements of Smart Grid are much more critical. Monitoring and controlling the generation and distribution of power is extremely critical and requires networks with extremely low latencies, very high reliability, availability and security, and communications in areas that may not be well covered by commercial networks. These elements of Smart Grid are best handled on an internal network specifically designed for and controlled by utilities. Using a commercial network open to consumers to carry information controlling generation and distribution presents a greater potential vulnerability for attacks on the nation's power grid.

Continued voice communications to ensure worker safety, transmit information to/from workers in the field to enable efficient and cost-effective operations, provide fast and efficient power restoration during outages and coordinate priority work with public safety entities during an emergency are also extremely critical. These communications functions should also remain on dedicated internal systems designed for the reliability, coverage and security required.

Utilities, like other enterprises and businesses, have received no additional spectrum allocations since Congress and the FCC implemented spectrum auctions. During this same period, demand for critical emergency communications has increased dramatically in the face of disasters. Federal requirements from the Department of Homeland Security, Energy Policy Act of 2005 and the Energy Independence and Security Act of 2007 to monitor and report critical infrastructure outages have increased utilities' requirements for reliable and secure communications.[6] While there is recognition of the link between potential terrorists attacks and the U.S. electric grid, action to support the communications requirements of this nation's electric utilities with additional spectrum is yet to be forthcoming.

[5] By examining the population density of counties nationwide, from highest to lowest based on U.S. census data from year 2000 Motorola calculates 98.5% population coverage would provide coverage to 63% of the geography. Alaska was excluded from the calculation because of its extremely low population density which would have skewed the results toward even lower percentages of geographic coverage if it had been included.

2. ***What are the basic requirements, such as security, bandwidth, reliability, coverage, latency, and backup, for smart grid communications and electric utility communications systems in general— today and tomorrow? How do these requirements impact the utilities' communication needs?***

Motorola takes the view that a utility's communications needs is the driver which impacts the requirements for network topology, security, reliability, availability, survivability, coverage, bandwidth, latency, backup, etc. Many of these requirements have already been addressed in the response to question 1, as the communications requirements and these network attributes are inextricably connected.

Communications networks are used primarily to protect against injury or loss of life, minimize any catastrophic equipment failures and provide reliable and cost effective electric service to utility customers. The general public and this nation's businesses will bear the inconvenience and cost of more or longer outages which can result from a lack of effective utility communications. The cost of such outages is well documented in a report issued by the state of California.[7] To minimize such outages and the efficiency of the electric utility's communications network, the following table summarizes general requirements for Smart Grid Distribution Automation (DA) deployments.

(Chart on Next Page)

[6] Energy Policy Act of 2005, Public Law 109-58, August 8, 2005, Sec.1839 on Transmission system Monitoring. Energy Independence and Security Act of 2007, Public Law 110-140, Dec. 19, 2007, Sec. 1304 re Smart Grid Technology Research, Development and Demonstration.

[7] PIER final project report, Value of Distribution Automation Applications, http://www.energy.ca.gov/2007publications/CEC-500-2007-028/CEC-500-2007-028.PDF, visited July12, 2010, at section 3.3.1.2, pages 60-63.

Smart Grid DA Hardware and RF Requirements	
Range	10 miles - rural deployments 5 miles - urban deployments
Latency	20 ms - maximum 1-way for a Smart Grid Access Point or base station operating at peak load for real-time control applications
Throughput	minimum: 500 Kbps aggregate Uplink/Downlink minimum: >= 100 Kbps Uplink throughput per Remote Module
Scalability	Minimum 200 Remote Modules per Access Point/Base Station
Data Performance	
	Protocols Support utility legacy protocols and convert to IP as necessary Distribution Automation legacy protocols (e.g., DNP3, GOOSE, Mirror Bits)
	QoS - Support high priority channel(s)
	Packets per Second (PPS) - 2,000 PPS - minimum
Certifications	IP67, IEEE1613
Media Access	Scheduled, synchronization method vs contention-based to achieve scalability and to limit self-interference
Environmental	Meet harsh environmental requirements for outdoor deployment in all 50 states
System Availability	Four 9's system availability with evolution to Five 9's
SCADA Interfaces	Support for transmission of SCADA protocols
Regulatory	FCC, comply with specific utility standards as required

3. ***What are additional considerations (e.g. terrain, foliage, customer density and size of service territory)?***

For all utilities, terrain, foliage, customer density and size of territory all play a role in defining the communications system requirement and solutions. These parameters of course will vary depending on the utility in question. Foliage is less of a problem in Arizona than in West

Virginia. Utilities also face additional environmental elements that must be considered in designing a communications system. For example, utilities in California must deal with earthquakes while those in the Gulf Coast states rather routinely face tropical storms and hurricanes. All utilities face the potential for severe thunderstorms or a terrorist attacks.

The one common element across all utilities is the need for reliable and cost effective communications networks designed to meet the respective needs in their areas. The availability of spectrum in various bands also plays into the solution chosen. For example, all other things being equal, signals in the VHF band generally propagate farther than those in the UHF, 800 MHz or 900 MHz bands. Therefore, VHF spectrum is highly useful in areas with lower population densities since better propagation helps minimize the cost of coverage. VHF spectrum may also be available in rural areas far removed from metropolitan and suburban centers. In contrast, in or near metropolitan and suburban areas VHF spectrum may already be fully licensed and therefore additional spectrum in that band is unlikely to be available for critical uses. The same is true of UHF spectrum.

The main reason that utilities look to private internal systems to meet their critical communications requirements is that commercial systems are designed instead to meet the needs of general consumers. As noted above, while this approach may be sufficient for AMI functions of Smart Grid, it is not compatible with utilities' more critical communications needs.

Commercial carrier systems are generally designed for low power, low antenna gain subscriber devices. Fixed site applications for Smart Grid can use high gain, directional antennas on the smart grid transceiver module, uncommon for public carrier system architectures. Also, as addressed earlier in these comments, commercial networks are often stressed during the periods when utilities need access to communications the most.

4. *What are the use cases for various smart grid applications?*

Use cases and communications requirements are being gathered in a number of forums. The SGIP (Smart Grid Interoperability Panel) has commissioned a study specifically to define wireless communications needs for the Smart Grid.[8] Earlier work by the OpenSG and documented in interim release 4.0 identifies 18 categories of use case for Smart Grid.[9] Generally, use cases cover three main categories: 1) account management and customer information; 2) operations, and 3) service restoration.

[8] Smart Grid Interoperability Panel (SGiP), NIST Smart Grid Collaboration Site, PAP02 :Wireless Communications for the Smart Grid (6.1.5), http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless, Visited July 12, 2010.

[9] SG Networks System Requirements Specification V4.0, http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Forms/AllItems.aspx, Open SG Users Group.

Account Management and Customer Information

Meter reading and customer information use cases are important but not as demanding as other utility applications from a communications perspective. Included in this category are service switching and service prepayment transactions. Going forward, this category will also include nomadic billing for plug-in hybrid electric vehicles. In this application category, delays in the delivery of information will not cause equipment damage or create an unsafe condition. Therefore, latency requirements are usually not as demanding as in other more critical utility communications functions.

The communications payloads can be a small as a few dozen bytes per transaction. Providing a customer friendly web interface could require payloads as large as a few hundred kilobytes. Aggregated meter data payloads from thousands of customers in a given area can grow to reach megabytes in size.

Operations

The operations category of use cases involves maintaining the safe and reliable operation of the energy delivery distribution network. Specific use cases include Volt-VAR define control, distribution switching and automation, load management and demand response. Communications to support the operations category tend to be more demanding from a reliability and latency perspective. Communications transmissions for these monitoring and control functions are not constant, but when needed must be available within fractions of a second. Delays introduced could cause equipment damage, unsafe conditions, or lead to system outages. Control messages in the operations category may need to be sent to thousands of devices simultaneously. Load management will take place during intervals of peak demand such as late afternoon and early evening.

Service Restoration

The service restoration category of use cases are very high priority and very demanding from a communications standpoint. Equipment damage is a possibility and protecting the safety of the workers and the public is essential when violent weather disturbs parts of the distribution grid. This can include thunderstorms, hurricanes, tornados, earthquakes and other natural disasters. Reliable communications is essential for fault detection and isolation. Reliable communications during outage intervals is essential for monitoring and controlling distributed generation resources. Latency requirements can be very short, in some cases, e.g., 20 milliseconds during faults when protection devices are switching. The increasing use of distributed generation means that going forward, there will be multiple energy sources feeding the distribution grid at multiple locations, further complicating service restoration efforts.

The Future

New technologies for distributed generation and renewable sources of energy will also create new use cases and related communications requirements. For example, California has a

mandate to increase renewable energy 33% by the year 2020 and an initiative to have one million solar roofs by the year 2018.[10] New Jersey has plans for 200,000 solar panels on utility poles.[11]

New technologies will increase fluctuations in the amount of energy flowing and the direction of energy flows in the distribution network. Today's power grid is one-directional. The future brings multiple power input points as multiple entities including consumers with stored wind or solar power who could sell power back to the utility. This creates a more complex control situation. These new Smart Grid use cases will introduce increased communications requirements to monitor and control the network.

Energy flows will be more variable over short time intervals with the introduction of wind and solar powered energy sources. Stabilizing the distribution grid with advanced communications will need greater bandwidths to accommodate and control the more rapid fluctuations in generated power. New uses cases are expected to arise as new technologies for distributed generation, islanding and microgrids, energy storage, and fine grained distribution grid phasor measurements become more mature.

The industry is also currently gathering additional detailed information regarding Smart Grid use cases and requirements for power distribution, Smart Grid IT, and communications.[12] Once this information is complete, it will provide additional insight for DOE initiatives.

As referenced in the NBP RFI, it is also important to remember that communications for utilities are not limited to Smart Grid applications. Essential utility networks in use today to ensure worker safety and efficient operation will still be needed for the foreseeable future. Converting these networks to broadband would require that more sites be deployed to provide equivalent coverage. In addition, there are no current plans to include direct unit-to-unit communications functions without infrastructure into 4G broadband radio standards. Direct unit-to-unit communications capabilities that exist in today's internal networks are essential for mission critical operations and the safety of utility workers.

5. ***What are the technology options for smart grid and other utility communications?***

Utility communications span a wide range of requirements today and the introduction of Smart Grid expands the overall complexity of needs. It is expected that multiple technology categories including wireless, wire-based, power line carrier and Ethernet will all be deployed to

[10] Executive Order S-14-08, http://www.gov.ca.gov/executive-order/11072/, and Schwarzenegger Signs Legislation to Complete Million Solar Roof Plan http://gov.ca.gov/index.php?/press-release/3588/, visited July 12, 2010.

[11] PSE&G Press release, PSE&G's "Solar 4 All" Program Approved, See http://www.pseg.com/solar4all/Attachments/July2909Solar4allrelease.pdf, visited July 12, 2010.

[12] Verizon, UTC do Smart Grid Homework, Washington Technology, http://washingtontechnology.com/articles/2010/06/21/smart-grid-study.aspx, visited July 12, 2010.

comprise the total solution. Wireless technology, both for internal dedicated utility networks and for commercial networks, will be an essential foundation for the total communications solution.

The mix of urban, suburban, rural, and deep rural requirements that utilities face, along with a variety of use-cases from AMI to high priority generation and distribution monitoring and control functions, dictates a mix of dedicated internal and commercial communications solutions for cost effective and safe operation. This may also include different frequency bands to support the mix of rural and metro, broadband and narrowband communications solutions required.

Wireless networks have widely varying characteristics depending on their operating frequency, power levels, antenna characteristics and locations, and the radio frequency environment (including interference environment). Utilities also have widely varying communications requirements that span from the need to cover hundreds of thousands of square miles down to covering repair operations at a given substation.

6. ***What are the recommendations for meeting current and future utility requirements, based on each use case, the technology options that are available, and other considerations?***

This has been addressed in the responses to previous questions. For customer information and meter reading use cases the communications needs are less demanding. Solutions based on a variety of networks, including commercial carrier networks, are being trialed today.

Operations and distribution management use cases require significantly lower latencies, must cover nearly all of a utility's service area and must be very secure to help protect against terrorism on the nation's power grid. Loss of communications will mean a loss in the ability to monitor and control the distribution grid which can lead to outages and severe consequences for businesses and the general public.

Service restoration use cases require mission critical communications networks that continue to operate during and after violent weather events. Real-time access to the grid's communications network is critical to a utility's workforce during such emergencies.

7. ***To what extent can existing commercial networks satisfy the utilities' communications needs?***

As noted in the previous responses, existing commercial networks may be used to satisfy some of the less critical communications requirements, including AMI. However, critical safety and control functions must have extremely high levels of guaranteed reliability, very low latency and specialized coverage that commercial networks do not provide.

The Utilities Telecom Council developed a whitepaper which addresses utility requirements.[13] Critical utility communications networks must be designed to accommodate peak communications loads that occur during an emergency. In the case of a dedicated network, utilities are in control of the specifications, design and operation, so these peak conditions can be accommodated. The goals of a utility network are to ensure the safety of personnel and infrastructure and the reliability of the electric service to millions of households. This is particularly important during natural or manmade disasters.

In contrast, commercial networks provide best-effort levels of service based on the requirements of consumers who comprise a much higher number of users than specialized operations like utilities. As noted on commercial carrier web sites with coverage maps, coverage is not guaranteed because it can vary over time and with traffic loading. Also, consumer traffic in an emergency situation can overtake and clog the system, leaving no access for utilities. As addressed previously in these comments, priority access would not guarantee a utility access on a clogged commercial system. It only places them first in line for the resource once an opening has been made by another user dropping off the network. While priority can be assigned, the shear number of general consumers trying to gain access to the system during a true emergency will would leave utilities with a very tenuous situation at best.

Utilities have four major success factors when designing utility networks: coverage, availability, capacity and functionality. These factors are potentially at odds with the design and business needs of a commercial carrier network. Coverage for utilities is not necessarily centered on the most populous areas of a region, and typically requires communications on 90% or more of the geography. In contrast, commercial systems are designed and specified as covering a percentage of the population, not the geography.

The Utilities Telecom Council has addressed utility reliability requirements:

> "…utility communications networks must withstand man-made and natural disasters, necessitating system design factors above and beyond those of a commercial provider's network. These systems must work "24 X 7, 365," to a "five 9s" standard of reliability (i.e. 99.999%), *especially* during service outages when other, commercial power-dependent systems are down."[14]

To meet that availability, built-in redundancy is a key requirement. However, this redundancy would likely generate unwanted cost for a commercial operator. Capacity to accommodate emergency situations that fluctuate as high as 500% or more above normal traffic levels is also required.

Utility communications network functionality must meet the need for timely, accurate communication, e.g., <20ms latency for protection relays. Stringent functionality requirements are likely to expand as Smart Grid systems grow and more intelligence is added.

---

[13] See *The Utility Spectrum Crisis: A Critical Need to Enable Smart Grids,* Utilities Telecom Council, January 2009.

[14] *See id.*, at page 9.

It is important to consider that the transmission and distribution of gas and electricity are provided to consumers "on demand" and can be extremely volatile requiring "real-time" control to be administered effectively and safely.

Furthermore, most commercial communications systems depend primarily upon utility-provided commercial power to maintain their systems. If power is interrupted, these communications systems will be interrupted as well which would have the effect of slowing progress on power restoration. Therefore, dependence by a utility on a commercial communications networks for more critical utility functions is unlikely to result in improved service to the public.

In short, eliminating the option for private internal utility networks would eliminate the ability of utilities to optimize communications systems to match their unique operational requirements.

8. ***What, if any, improvements to the commercial networks can be made to satisfy the utilities' communications needs?***

As noted in these comments, a commercial network can partially satisfy the needs for communications by supporting functions that are non-critical. The description of a utility's more critical communications requirements and the current commercial network shortfall in meeting those requirements as addressed in the response to question 7 provide insight into what would need to be changed.

While modifying commercial system to provide the requisite level of guaranteed availability across a utility's overall geography may be theoretically possible, we doubt it is viable from a business standpoint. Doing so would significantly raise the cost to all users on the system when only a few would actually need the increased reliability and coverage. This would place any commercial operator who chose to do so at a disadvantage to other commercial operators who do not make the substantial changes required.

The following summarizes changes in commercial systems that would be needed to accommodate the critical communications requirements of utilities:

- Design to cover the geography of utilities rather than the population based coverage as in today's commercial systems;

- Guaranteed coverage, availability, and reliability under contract provisions, possibly including liability clauses if communications outages lead to damage of power grid equipment or injury/death of utility workers;

- Backup power, including redundant gear and batteries for several days operation to ensure operation throughout the coverage area, not just at some cell sites;

- Pre-emption of consumer customers to ensure utility access during critical events and service restoration;

- Special provisions to allow utilities the transparent control for monitoring applications required for their operations;

- Provisions to accommodate information flow directions that may differ from consumer use;

- True multicast so utility users can communicate as a group when needed, rather than just one-to-one communications;

- Reasonable pricing to accommodate unlimited access utilities will need in an emergency situation for power restoral functions; and

- Special interfaces to connect its wireless communications networks to a utility's dispatch console system, mobile data system and SCADA systems.

Obviously, from a commercial system business perspective, it would be uneconomic to apply many of these requirements to serve the unique needs of a relatively small subset of users, even given these users' critical role.

9. ***As the Smart Grid grows and expands, how do the electric utilities foresee their communications requirements as growing and adapting along with the expansion of Smart Grid applications?***

Capabilities that have never been seriously considered before will become feasible if reliable Smart Grid communications become available. This is likely to lead to applications that are not foreseen today, but emerge as utilities gain experience in deploying and using Smart Grid tools. The key is to provide a sufficient foundation and flexibility to accommodate these as yet unforeseen applications. This includes spectrum capacity for dedicated utility communications and rules that leave operational decisions to utilities.

<u>An additional Issue-Security</u>

While not specifically addressed in the NBP RFI, we think it is also important to consider additional security requirements that emerge as Smart Grid system are developed and deployed. NERC-CIP standards (NERC-CIP 001-009) and the NIST Guide to Industrial Control Systems Security (SP 800-82) are high-level documents that contain requirements guidelines. More work is needed to create a comprehensive set of security requirements relevant to the generation, transmission and distribution aspects of the Smart Grid.

Smart Grids will require greater network connectivity to support the new, more sophisticated features of power grid control systems. The addition of remote system management, distributed intelligence and more accessible communications has the potential to open the grid to new threats. A comprehensive security solution would include layers of defense to minimize the threats from interruption, interception, modification and impersonation. Appropriate incident response plans and consistent security policies are also required at a network management level to ensure the security of the Smart Grid.

The security of the grid will depend on authentication, authorization and privacy technologies. Privacy technologies are generally mature (e.g. FIPS approved AES). Many established security technologies rely on key management. The Smart Grid will rely on millions of devices, spread across multiple organizations requiring an approach that is highly scalable while supporting the highest possible levels of efficiency to ensure that unnecessary costs due to overhead, provisioning and maintenance are minimized.

It is likely that new key management systems, specialized to meet the requirements of Smart Grid, will be needed. In our view, the most effective solution for securing the Smart Grid will be based on public key infrastructure ("PKI") technologies. While PKI is complex, this can be managed by the use of four main technical elements: PKI Standards, Smart Grid PKI Tools, Trust Anchor Security and Certificate Attributes.

In summary, a Smart Grid solution should consider the following security features to protect the integrity of the network:

- Subscriber module authorization and authentication;
- Multiple levels of access and change permissions for administrative users;
- Capability to lock down/inactivate all unused ports and protocols as part of the overall platform security strategy;
- Security Logging to track login attempts and configuration attempts;
- Password strength and aging rules;
- Secure management protocols (SNMPv3, SFTP, HTTPS, TLS); and
- 128 bit AES encryption with FIPS-197 certification as standard mode of operation.

A comprehensive solution including reliable methods for confidentiality, integrity, authentication, authorization, access control, availability and non-repudiation must be incorporated into the Smart Grid at a network or device level.