

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of Smart Grid	)	GN Docket No. 09-47
Technology, NBP Public Notice #2	)	GN Docket No. 09-137
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51

**COMMENTS OF MOTOROLA, INC.**

Motorola, Inc. (“Motorola”) respectfully submits these comments in response to the Commission’s Public Notice concerning Smart Grid technologies and solutions.<sup>1</sup> This Public Notice seeks comments on how advanced infrastructure and services could help achieve efficient implementation of Smart Grid technology, and is a follow-up to more general comments received in response the Broadband Plan NOI.<sup>2</sup>

Motorola appreciates the Commission’s focus on enabling Smart Grid solutions, as part of the larger review of broadband policy issues. Motorola previously addressed many of the issues raised in the Smart Grid PN in its comments to the Broadband Plan NOI and urges the Commission to review these further comments in conjunction with those previously filed.<sup>3</sup>

---

<sup>1</sup> Comment Sought on the Implementation of Smart Grid Technology, Public Notice, DA 09-2017, released September 4, 2009 (“Smart Grid PN”)

<sup>2</sup> A National Broadband Plan for Our Future, Notice of Inquiry, GN Docket No. 09-51, FCC 09-31 (2009) (“Broadband Plan NOI”).

<sup>3</sup> Comments of Motorola, GN Docket No. 09-51, submitted June 8, 2009.

## **I. Smart Grid Solutions.**

The Smart Grid PN raises a series of questions regarding Smart Grid technology and solutions. These questions fall into five categories: (1) communications networks and technologies suitable for various Smart Grid applications; (2) the availability of existing communications networks and associated impact on Smart Grid deployments; (3) how public and private wireless spectrum is or could be used for Smart Grid applications; (4) the benefits of real-time consumption and pricing data; and (5) details regarding home area networks, including security.<sup>4</sup> We believe that public utilities are in the best position to provide input on real-time consumption and pricing data so these comments will focus on the other four categories of questions.

### **A. Networks and Technologies Suitable for Smart Grid Applications.**

Noting that Smart Grid applications are being deployed using a variety of public and private communications networks, the Commission states that it seeks to better understand which communications networks and technologies are suitable for various Smart Grid applications.<sup>5</sup> There is no single public or private Wide Area Network (WAN), that provides the utility industry or marketplace with all the capabilities needed to implement viable Smart Grid solutions. A comprehensive strategy that takes into account the needs of multiple current and planned intelligent grid applications will require a combination of solutions in order to achieve sound technical, operational, reliability, security and financial goals. Further, the requirements and solutions

---

<sup>4</sup> Smart Grid PN at 1-4.

<sup>5</sup> *Id.* at 1.

applicable to residential aspects of the Smart Grid may be different from those applicable to the core part of the network used to control generation and distribution.

Properly designed private networks provide a high level of security and reliability and lower latency, and will be especially important for core generation and distribution functions. In contrast, public networks may be more cost-effective than a dedicated private network for some elements of the Smart Grid where an assured high level of reliability, security and low latency is less essential, or may facilitate connecting into every residence. In addition, while many intelligent grid applications will require broadband, basic advanced meter infrastructure (AMI) functions like remote meter reading can be accommodated on lower bandwidth networks with significantly lower data rates. As AMI becomes more advanced, however, data rates for those elements will increase.

For wireless solutions, coverage from any single transmitter generally shrinks as data rates over the channel are increased, so it is essential to understand the requirements of various elements of the overall Smart Grid solution to arrive at cost effective approaches. While the focus of this proceeding is primarily on broadband, Motorola therefore urges the Commission to enable a comprehensive set of Smart Grid solutions based on the relevant requirements. The various key functions and their high level requirements are addressed below. Detailed technical requirements for Smart Grid solutions are still under development.

Because technology selection should be based on requirements, it is premature to select specific technologies at this time. Also, to enable cost-effective solutions with economies of scale, the best technology will depend in part on the spectrum identified

and made available for Smart Grid solutions. For example, if Smart Grid communications were to be accommodated at 700 MHz, LTE would be a broadband technology for serious consideration. In contrast, if the spectrum identified for Smart Grid deployments in the United States were at 2.5 GHz, WiMAX may be a more appropriate technology to consider. By considering the overall attributes and requirements of different communications elements of the Smart Grid, spectrum options can be developed in advance of finalizing selection of specific communication technologies.

AMI applications are the first Smart Grid technology application that is most visible to consumers as it will be used to inform smart devices in the home and business when energy demand is high and track how much energy is used and when it is used. Initial AMI applications are characterized by a requirement for delay-insensitive, low bandwidth, non-real-time communication links. Based on these requirements, AMI deployments in the industry are utilizing both unlicensed and public carrier systems to implement trials and early deployments.

AMI is just one element to enable the success of Smart Grid solutions. To achieve significantly improved reliability, efficient electricity delivery, reduced outage and reduction in overall energy usage, a unified communications network for power generation and distribution systems will also be required. Communications systems that control power generation or delivery methods will be held to very high standards to ensure the safety of utility workers and the public. Proper functioning of the communications network will be required for reliable and safe operation of the electric power grid. As such, the communications networks will need to be secure against

intrusion, intentional disruption and accidental failure. Control of power generation and distribution therefore will require a highly reliable, secure communications network with very low latency and assured performance.

Any communications network designed for these Smart Grid generation and distribution applications must be robust and resilient during severe weather, environmental events and outages in the electric power grid itself. In addition, this network must be designed with the capacity to continue to operate under worst case conditions. The network must be as free as possible from intentional or unintentional interferers. Communications will also be needed both in heavily populated areas and in areas far from population centers where generation and distribution assets may be located. In parallel with the data and machine-to-machine communications among generation and storage devices, distribution devices and loads, mission critical voice communications are also needed to ensure the safety and efficiency of utility workers.

While some AMI functions may be operated over unlicensed spectrum or commercial systems, the attributes of communications for generation and distribution are likely to require dedicated spectrum for private networks, in addition to wired broadband connectivity.

Trials and early deployments underway will help to define and confirm Smart Grid solution requirements. For example, Motorola is joining in partnership with the Horizon Energy Group (HEG), together with the host utility, San Diego Gas and Electric (SDG&E), and its teaming partners Advanced Control Systems (ACS), Science Applications International Corporation (SAIC), Pacific Northwest National Laboratory (PNNL), and the University of San Diego (USD) to propose an integrated GridWise

pilot-project which will be implemented on selected SDG&E feeders/substations.

Motorola has overall responsibility for communications to support this trial.

**B. Availability of Existing Networks and Impact on Smart Grid Deployments.**

Given that electric utilities offer near universal service, including in many geographies where no existing suitable communications networks currently exist, the Commission seeks to better understand the availability of existing communications networks, and how this availability may impact Smart Grid deployments.<sup>6</sup>

For most Smart Grid applications conducted at commercial or residential premises, network connectivity must be continuously available to the Smart Grid application. This precludes reliance on dial-up types of communications circuits because most communications would be initiated from the utilities' centralized facilities rather than from the home. Therefore the percentage of homes without access to dedicated fixed always on internet connectivity, whether wireless, telephone line (DSL), fiber to the premise, or cable is arguably the percentage with no suitable communications network access for AMI functions. This assumes that this type of commercial network is suitable for Smart Grid AMI applications, an assumption which may be valid primarily for simple meter functions.

As noted above, core generation and distribution functions require a higher level of reliability and security, as well as lower latency than AMI and would require a Private Network. Therefore, we do not believe the availability of commercial networks is as relevant a factor for generation and distribution elements of the Smart Grid.

---

<sup>6</sup> *Id.* at 2.

### **C. Public and Private Spectrum for Smart Grid.**

The Smart Grid PN asks how wireless spectrum is or could be used for Smart Grid applications.<sup>7</sup> There is currently insufficient spectrum to accommodate Smart Grid generation and distribution solutions going forward. Requirements surrounding latency, backbone peak data rates, advanced meter interrogation (future-looking) and consumer premise control cannot be accomplished using narrowband spectrum that is currently being used to support critical voice functions.

Some of these applications can be addressed using powerline networking technology, but it is unlikely to satisfy all the requirements. For wireless solutions, many needs could possibly be met using wideband channels (*e.g.*, 100 kHz to 1 MHz in bandwidth). However, most technology development for data is now focused on broadband, using channels that are at least 5 megahertz in bandwidth. Also, there is no spectrum available for private point to multipoint applications that could provide reasonably sized coverage “cells” (*i.e.*, 5 to 20 km). The use of unlicensed spectrum is expected to be limited as requirements for reliability/availability, security and longevity argue for the use of licensed spectrum except for certain non-critical needs such as meter reading.

Since the mid 1990’s, the FCC’s spectrum policies that strongly favor auctions as a licensing approach have resulted in a lack of sufficient spectrum for mission critical and business critical internal communications systems. There has not been an allocation of spectrum geared for internal industrial or utility use since the 900 MHz band was

---

<sup>7</sup> *Id.* at 2, 3.

allocated in the late 1980s.<sup>8</sup> Decades have passed and utilities, as well as other enterprises that rely on internal communications systems for the safe and efficient operation of their businesses, which provide economic growth and security for the county, have struggled to keep pace with increasing communications requirements. The lack of dedicated spectrum, resulting in the need for these utilities and business to rely on commercial broadband networks that may not fully meet the needs of utilities and businesses, make deployment of secure, reliable Smart Grid solutions nearly impossible.

The Utilities Telecommunications Council (UTC) estimates that an additional 30 MHz of spectrum is required for new data applications such as Smart Grid, as well as for expanded critical mobile voice operations for utilities.<sup>9</sup> UTC indicates that two-thirds of this estimate (i.e., 20 MHz) is needed for high speed data to support AMI, Smart Grid implementation and security and vehicular data. The remaining 10 MHz is needed for voice dispatch. Motorola has reviewed the UTC report and agrees with its recommendations.

In addressing questions on spectrum, the Commission also raised questions regarding coverage, throughput and latency requirements.<sup>10</sup> Coverage of signals at acceptable data rates in rural areas is a real concern. While carriers provide good coverage for the consumer market, utilities often require coverage in remote areas where the data rates and coverage of commercial systems will be significantly less. Within rural

---

<sup>8</sup> See e.g., *Allocation of 900 MHz Spectrum Reserve for Private Land Mobile Radio Systems*, Report and Order, Gen. Docket No. 84-1233, 2 FCC Rcd. 1825 (1986).

<sup>9</sup> The Utility Spectrum Crisis: A Critical Need to Enable Smart Grids, Utilities Telecommunications Council, January 2009 at Section V.

<sup>10</sup> Smart Grid PN at 3.

areas, as one travels away from interstate highways or clusters of population in a town, actual coverage may not be present. Coverage in these rural areas for smart grid operations is likely to be increasingly important as the country moves to using alternative power sources, such as wind and solar farms that are located away from population centers.

Data rate requirements of utilities would often tend to coincide with peak consumer use periods. Peak drive time would correlate to time-of-day where load shedding, device control, and other Smart Grid needs would also peak. Furthermore, at times of power outages, communications usage requirements of utilities and consumers will also tend to peak together. Combining these peak loads on a single network could result in suboptimal operation of the smart grid as well as degraded service for consumer devices. Connectivity should include intelligent electronic devices and control of consumer and commercial devices/loads connected post-meter. The Smart Grid system should be planned to accommodate an expected growth in number of such devices.

Some data transfer, such as meter reading, can be deferred to off-peak hours. However, if control of the grid to disable devices on a per-meter basis is required, data usage is likely to soar beyond that which can be handled by commercial systems. The problem would be even worse when an emergency occurs that will stress all aspects of a commercial system.

Latency requirements vary considerably; meter reading of commercial utility services may take place on a quarter hour basis while hourly readings may be sufficient for residential meters. However, control of post-meter intelligent electronic devices need to take place in a more timely fashion – perhaps in seconds – if load shedding is to be

considered effective. On the other end of the latency spectrum, command and control of some classes of devices require latencies of fewer than 20 milliseconds (“ms”) and there are critical devices that require 4 ms latency or less. Finally, future use of “synchrophasors<sup>11</sup>” to detect, anticipate, and allow feed-forward corrective action to take place will also require latencies below 20ms.

Currently, no narrowband or unlicensed solution exists that has the coverage range to meet this need. Furthermore, under the current deployment, low-latency, high criticality needs are met with wired lines such as T1 level service. These services provide a point of vulnerability from the standpoint of homeland security as well as a source of great expense for the utility. These costs are passed to the consumer; however, cost to the consumer can be reduced and reliability increased through the use of dedicated spectrum.

Harmonization of spectrum allocations between the US, Canada, and Mexico would provide a means to control, with proper security attached, the purchase and sale of power over international boundaries. In particular, the US purchases considerable excess generation capability from Canada and harmonization of control through coordinated spectrum would be ideal. Canada has identified the 1800 to 1830 MHz band for primary use by utilities. In the U.S., this band supports Federal Government and Department of Defense systems that would be difficult to relocate.

The Commission also asked about the need for paired spectrum allocations. For Smart Grid data operations, TDD or FDD solutions could be utilized. However, as noted

---

<sup>11</sup> Synchrophasors are precise grid measurements available from monitors called phasor measurement units (PMUs). Synchrophasors enable a better indication of grid stress, and can be used to trigger corrective actions to maintain reliability.

previously, the choice of technology will be made in part because of economies of scale. This means that neither paired nor un-paired spectrum should be ruled out at this time.

**D. Smart Grid Security.**

As part of its inquiry into spectrum requirements, the Smart Grid PN raised questions about the security of the network as well as privacy and security concerns about personal information.<sup>12</sup> The Smart Grid aims to make electricity distribution more intelligent and digitally-based. The threat of hackers causing blackouts, stealing sensitive information, or rerouting power loads raises concerns over the availability, confidentiality, and integrity of the Smart Grid. As a result, the cyber-security of the solution is paramount and should be a primary focus. Security defenses should be incorporated from the very beginning and should stretch across the entire framework of the Smart Grid implementation.

Incorporating security into the solution requires planning, so as not to stifle innovation. To reduce the intrusive impact of security, it is recommended that security be built-into the solution from the very beginning. This built-in approach would allow end-to-end security in a way that is consistent throughout the network. In addition, it will ensure that developers and device-makers all work from the same standards, thus eliminating incompatibility issues. Standardization of the built-in security would minimize vulnerabilities within specific applications or devices. Today's networks are riddled with vulnerabilities that vary across the network due to the lack of built-in security in many applications and devices. This should not be the model for a network as

---

<sup>12</sup> Smart Grid PN at 3.

important as the Smart Grid. Layers of defense should be built into the solution to minimize the threats from interruption, interception, modification, and fabrication.

The sharing of Personally Identifiable Information (PII) gathered from the Smart Grid raises concerns over privacy. What information and how it's retrieved from the various end-points should be well-defined and regulated to maintain the privacy of its users. Intelligence can be collected to improve efficiencies of the system, assisting both power companies and their customers. However, approaches to gather this intelligence should be carefully reviewed to ensure that it's collected and stored in a secure manner. Customers should have the ability to opt-out of providing PII information that could be used by an adversary to target that individual or company. For example, this data could include information about a particular customer who suddenly has extremely low power usage. This could be a possible indication that the individual is away on vacation. In the wrong hands, this could make that house a target for a robbery, since the PII would also include their name and address. Therefore, where and how the data is used should be carefully reviewed and defined. Statistical data should be shared in an anonymous manner to those who are responsible for evaluating and redistributing loads.

Keeping the network private would greatly minimize the threats from intruders. An Internet-based Smart Grid approach, as commonly found with commercial networks, opens the grid to threats from multiple types of attacks. These include geo-political threats such as a cyber attack from a terrorist group looking to cause an interruption to the power supply. Another type of attack is worm infestations which have proven to negatively impact critical network infrastructures. Such threats have largely been the result of leaving a network vulnerable to threats, usually from the Internet. For example,

there have been denial of service (“DoS”) attacks on a single network that disrupted all directory name server (“DNS”) thus prohibiting users from connecting to any of the resources. This demonstrates the fragility of an Internet-based commercial network.

The components, systems, networks, and architecture are all important to the security design and reliability of the solution. But it’s inevitable that an incident will occur at some point and one must be prepared with the proper Incident Response plan. This can vary between commercial providers and private utility networks. A private utility network is likely to provide better consistency of the incident response plan in the event of a security incident, assuming the private network is build upon a standardized framework of hardware and software. The speed of the response decreases exponentially as the number of parties involved increases. Conversely, a private network would ideally depend on fewer parties, therefore a more efficient incident response process would provide for more rapid response and resolution. The rapidity of the response is critical during situations that involve a blackout. A private utility network also generally requires more specific knowledge to manage or attack, so it would be more secure. Criticalness of the device or system also determines how prone it will be to attacks. History has shown that private networks by their inherent nature are less prone to attacks, and as a result are recommended as the best approach in situations where security is paramount.

## **II. Summary**

There is not any single public or private Wide Area Network (WAN), that provides the utility industry or marketplace with all the capabilities needed to implement viable Smart Grid solutions. The Commission and industry need to develop a

comprehensive strategy that takes into account the needs of multiple current and planned intelligent grid applications and develop solutions that can achieve the technical, reliability, security and financial goals which must be met to serve the American public with an effective Smart Grid. Simple AMI functions can be supported by unlicensed or commercial licensed networks. More critical areas of communications to support generation and distribution will require higher levels of reliability, security and the lower latency levels that private dedicated spectrum and systems typically incorporate. We look forward to participating in Smart Grid trials to further define the requirements and optimum solutions.

Respectfully Submitted,

/s/ Steve B. Sharkey

Steve B. Sharkey

Senior Director

Regulatory and Spectrum Policy

Motorola, Inc.

1455 Pennsylvania Avenue, NW

Washington, DC 20004

TEL: 202.371.6900

October 2, 2009