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	)

REPLY COMMENTS OF MOTOROLA, INC.

Motorola, Inc. ("Motorola") hereby submits reply comments to the National Broadband Plan Request for Information ("RFI") on the communications requirements of utilities, including but not limited to requirements for Smart Grid.[1] Motorola previously submitted extensive comments to the RFI which examined the communications requirements for Smart Grid and other key utility functions and recommended the solutions most applicable to various utility requirements.[2] As addressed in those comments, 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. The comments in the proceeding from other entities who have first hand knowledge of utility requirements made similar recommendations.[3] Separating the generation and distribution elements from the "consumer-facing" functions in the overall Smart Grid network also 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.

2 Motorola Comments dated July 12, 2010 in response to Department of Energy RFI.

3 For example, see comments of Utilities Telecom Council.

I. Summary of Motorola's Key Recommendations

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

1) Utilities' operational requirements should be the primary foundation for DOE decisions and recommendations to sister Federal agencies. Smart Grid communications needs can be broken into its component key elements to address requirements and viable solutions. For example, advanced meter infrastructure is a somewhat less critical function that tolerates higher latencies and should be accomplishable in metro areas over a commercial network. 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.[4] 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.

2) 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.

3) 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.

4) 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.

5) 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. It is likely that new key management systems, specialized to meet the requirements of Smart Grid, will be

[4] As addressed in Motorola's comments, covering a certain percentage of the population is significantly different from covering a similar percentage of the geography.

needed. 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.

6) 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. The option to choose a dedicated private internal system is an essential part of that decision-making process.

II. Conclusion

Motorola supports the RFI initiative by the DOE to help determine utilities' communications requirements for Smart Grid, as well as other key functions. Motorola has provided significant information on utility communications requirements and recommendations to meet those requirements. These recommendations provide a framework within which to move forward with a reliable, secure and viable Smart Grid communications network.

Respectfully submitted,

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

August 9, 2010