Prepared Statement for Mr. Michael P. Mertz
Director, NERC Regulatory Compliance
PNM Resources, Inc.
US Department of Energy – Quadrennial Energy Review Meeting
August 11, 2014

Thank you for the opportunity to participate in the Quadrennial Energy Review. I am Mike Mertz, the Director of NERC Regulatory Compliance at PNM Resources, a role that includes oversight of our Critical Infrastructure Protection program. PNM Resources is the holding company for two utilities- PNM and TNMP- that collectively serve nearly three-quarters of a million customers in New Mexico and Texas. We are the only publicly-traded company headquartered in New Mexico.

I appreciate the opportunity to speak to the topic of future energy systems and addressing the vulnerabilities of our nation's energy infrastructure. The electric grid represents one of the most complex and robust machines ever created. Several, if not all, other critical infrastructure sectors depend on the reliable operation of the electric system to perform their essential functions. As an electric utility involved in ensuring the reliability and security of the North American grid, we are concerned not only about the significant traditional risk landscape such as extreme weather and aging infrastructure, but also with existing and emerging risks in both the physical and cyber security arenas.

Threat and Vulnerability Management-

Like others in the energy sector, PNM Resources remains vigilant in ensuring the protection of our assets. Our commitment to the customers we are privileged to serve demands nothing less. Threats to the reliable operation of our grid are constantly growing and rapidly evolving. As a result, we are continually refining and adapting our programs to quickly detect vulnerabilities, and protect our systems from a wide variety of threats ranging from coordinated nation states, to sophisticated cyber criminals, to individuals with malicious intent. Certainly the events of last several years have caused both industry and government to reassess the security of the

grid, recognizing the need to enhance physical and cyber security measures, and to accelerate investments to build additional resiliency and security in our systems.

For protection against both physical and cyber threats, PNM Resources uses a defense in depth strategy with controls and policies aligned with the same standards used by the federal government. Our security strategy is aimed at protecting our critical infrastructure; ensuring the confidentiality, availability and integrity of our data; and ensuring the operational continuity of our electric systems. Our comprehensive approach to protecting our systems and facilities includes many different elements, including access and authentication controls, physical and cyber intrusion detection capabilities, network protection, malware prevention and e-mail filtering. Tools deployed to closely monitor our assets also give us the capability to evaluate the threats as they evolve and adjust system protections, while internal and external audits and assessments provide ongoing evaluation of our protective measures. People also serve as an integral part of our program and all of our employees receive regular cyber security training, with many receiving role based training such as the Control Systems Security training programs offered through the Department of Energy National SCADA Test Bed.

Partnerships-

Beyond protecting our infrastructure, effectively sharing timely information with other utilities and federal agencies is critical to providing our customers with reliable, affordable, and secure electricity. As threats become more sophisticated, we need to foster additional public-private partnerships while expanding existing outlets to further provide coordination between government and private sector. PNM cyber and physical security staff communicate on a regular basis with government agencies, law enforcement, and industry peers to assess the threat environment, and we seek out opportunities to promote information sharing. Earlier this year, PNM hosted a joint DOE/DHS sponsored *Electric Substation Security Awareness Campaign* in Albuquerque that brought together government partners, law enforcement, and industry experts to share threat information and best practices in the utility substation environment. We also recognize that threats are not scaled based on the size of the organization, so we initiated an effort to reach out to smaller electric co-ops, municipalities,

and local businesses, hosting a *NM Cyber Community Workshop* this spring that included resources from around the state of New Mexico as well as security experts from DHS, FBI and DOE. When it comes to infrastructure protection and information security we have some of the leading industry experts right in our own back yard, so we are currently working to establish a memorandum of understanding with Sandia National Laboratories to further promote information sharing and best practices. Although our company continually assesses risks and improves its security posture to align with new and emerging threats, the federal government, with sophisticated intelligence-gathering capability, is best positioned to help identify, evaluate, and communicate threats, while providing assistance in defending our systems and infrastructure from coordinated criminal and nation state threats.

Policy-

The changing nature of threats and vulnerabilities also makes it difficult to address cyber and physical security from a policy perspective. Where federal policy is necessary we must ensure that any standards for the private sector do not inadvertently prevent new technology, but rather promote investments while providing utilities a clear path for rate recovery. We must also be careful to avoid attempts to develop standards targeted to only specific threats or vulnerabilities, and to ensure they are technology agnostic, as reactive policy simply cannot keep up with the cyber threat landscape. Today, the electric and nuclear sectors are already subject to mandatory and enforceable Critical Infrastructure Protection standards that address both cyber- and physical-security. Long before the Federal Energy Regulatory Commission's (FERC) approval of the Critical Infrastructure Protection standards in 2008, we were planning and implementing a wide variety of additional steps to protect essential systems and other key elements of the grid. PNM Resources shares FERC's concerns outlined in a recent directive to develop additional physical security standards for critical infrastructure, and we will continue to be active participants in the standards development process to achieve those goals. The FERC directive also reflected our view for all standards development, that system owners and operators should have considerable flexibility in implementing protective measures, based on their familiarity with their own service areas, assets, and the unique qualities of their

customers. The one-size fits all approach simply does not work in the security realm. Where standards must exist, we need to continue to work together to ensure they allow the private sector the flexibility to implement the appropriate risk based measures necessary to fulfill our obligation to the customers we are privileged to serve.

Closing-

In summary, the electric grid is an extraordinarily complex machine that continues to evolve and adapt with new technology. It supports nearly all other critical infrastructure that we rely on for the safety and security of our nation, and it touches nearly every element of our daily lives. But the grid is not immune to existing and emerging physical and cyber threats. While we implement a wide variety of controls to protect our assets, many threats are best addressed through public/private partnerships, rather than prescriptive policy. We applaud the many efforts underway at DOE aimed at improving security of energy delivery systems and we believe these existing partnerships should be expanded to allow for better information flow between the private sector and government. New partnerships should also be explored to support financing mechanisms for resiliency and security investment, and government policies should be shaped to provide regulatory certainty, so that utilities can continue to maintain a resilient, modern, and secure grid. Thank you for the opportunity to participate in the QER process.