DUPONT SUMMIT 2013

Pressing Issues, Economic Realities

December 6, 2013 * Historic Whittemore House, Washington, DC

The Policy Studies Organization

Speaker

Rita Wells – *Idaho National Laboratory*

"Compliance Cyber Security Limits Innovation in Cyber Defense of Electric Infrastructure"

Years of resources applied to reducing cyber security fines by the electric industry has resulted in slow adoption of defensive performance based measures to secure our most critical of infrastructures from cyber attacks. Current cyber security standards for the electric grid are compliance based and not inclusive for all entities, leaving vulnerable interconnected architectures and interdependencies with other infrastructures exposed (Federal Powers Act 2005 section 215 created the Energy Reliability Organization). The North American Electric Reliability Corporation (NERC) serves as the ERO with an open and static compliance driven cyber standards which favor the auditable requirements instead of performance based cyber controls needed to respond to the agile dynamic nature of the cyber threats. The open standards process is too slow to incorporate new defenses. Performance based cyber controls allow for continual process improvement for industry and stronger defense for the energy sector with security improvement benefits for non-regulated entities as well. This policy shift would move the focus to defense and agile response as compared to the current compliance paper trail to reduce punitive fines on these requirements. Technologies exist to defend against the creative agile cyber attacks in the energy sector. Policies, and punitive compliance based cyber standards in the electric sector have had unintended consequence with utilities not using newer agile defense techniques due to the cost of the auditable paper trail needed to implement. With over 4,000 entities involved in the generation, distribution and transmission of electricity, the inner connected nature provides cyber pathways for attack with limited information sharing when events occur. Oil and gas transmission and delivery systems are not subject to a central cyber security requirements and no information sharing capability. The U.S. government has been asking energy asset owners to protect for a nation state cyber attack without a business case or common rate recovery capability. Further complicating this issue is the inclusion of infrastructures outside the U.S. boundaries that the U.S. relies on for energy.