Testimony of Barbara Sugg

Vice President of Information Technology and Chief Security Officer

Southwest Power Pool, Inc.

Member, Information Technology Committee, ISO/RTO Council

Before the House Committee on Energy and Commerce

Subcommittee on Energy

"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

February 1, 2017

Executive Summary

- ***ISO/RTO Council (IRC):*** The IRC is made up of nine Independent System Operators and Regional Transmission Organizations (ISO/RTO) in North America serving two thirds of electricity consumers in the United States and over half in Canada. The IRC and its committees bring together representatives from each ISO/RTO to work together to match power generation instantaneously with demand to keep the lights on and ensure access to affordable, reliable and sustainable power via wholesale energy markets.

- ***CIP Standards:*** The Critical Infrastructure Protection (CIP) Standards have been maturing since first approved by the Federal Energy Regulatory Commission in 2008. These mandatory standards provide for a robust, base level of security for which all utilities, including ISO/RTOs, must adhere. The CIP Standards cover numerous domains of cybersecurity, including, but not limited to, identifying cyber assets, controlling access, managing changes, addressing vulnerabilities and protecting information.

- ***Culture of Security:*** Each ISO/RTO acknowledges cybersecurity as their top corporate risk. Our core cybersecurity strategies focus on the key principles of Defense, Response, Recovery, Partnership and Education. Our security programs must continue to reflect more than that which is required by the standards.

- ***Defense in Depth:*** The IRC is committed to collectively supporting the resiliency efforts of each ISO/RTO. While system redundancies are necessary requirements, ISO/RTOs also maintain close ties to the utilities they serve, as well as their neighboring regions thus allowing for immediate operational assistance and threat mitigation in the event of a cyberattack.

- ***Response, Recovery, Resilience:*** ISO/RTOs routinely practice cyber incident response and system recovery to ensure resilience in the wake of a cyberattack. Drills are routinely conducted on local, state, regional and federal levels, in coordination with government agencies and industry associations to provide opportunities to improve our ability to respond and recover with the goal of maintaining the highest possible level of resilience.

- ***Conclusion:*** It is essential that the electric industry continue to prioritize cybersecurity maturity above and beyond that which is required for compliance as the evolving threats and emerging technologies are surfacing faster than standards can be contemplated and promulgated. While the standards themselves are indeed robust, we must not be complacent in our efforts to protect the bulk electric system from cyberattacks and must continue to maintain reliability and resiliency for the American people.

Good morning Chairman Upton, Vice Chairman Olson, Ranking Member Rush, and members of the Subcommittee. Thank you for holding this hearing concerning the electricity sector's efforts to respond to cybersecurity threats. My name is Barbara Sugg and I am the Vice President of Information Technology and Chief Security Officer at Southwest Power Pool Inc. (SPP) headquartered in Little Rock, Arkansas. SPP is one of nine Independent System Operators and Regional Transmission Organizations (ISO/RTO) in North America that make up the ISO/RTO Council (IRC), established in 2003. I am testifying before you today, as the designated representative of the IRC, about the requirements and responsibilities of ISO/RTOs in protecting the bulk electric system in North America from cyberattacks, as well as responding to and recovering from such an event.

The IRC serves two-thirds of electricity consumers in the United States and more than half in Canada, spanning three interconnections. ISO/RTOs match power generation instantaneously with demand to keep the lights on and ensure access to affordable, reliable and sustainable power via wholesale energy markets. ISO/RTOs provide a variety of services to their diverse groups of members, including serving as North American Electric Reliability Corporation (NERC) certified Reliability Coordinators, Balancing Authorities, transmission planners, open access transmission tariff administrators, and wholesale energy market operators.

By sharing innovative ideas and best practices, IRC members work together to build a smarter and more efficient and secure electric grid that is well prepared to serve the North American power market and its consumers, today and in the future. As a collective group, the IRC consists of an Executive Committee, comprised of the chief executive officers from each ISO/RTO, as well as numerous committees responsible for supporting the IRC's goals and initiatives. These committees share information across a wide range of important areas, including potential physical and cyber threats, regulatory and legislative issues, standards development, transmission planning, market standardization and information technology. Across the numerous IRC committees, staff from each ISO/RTO routinely work together in a collaborative, open and transparent manner within the framework established by the IRC.

For the past nine years, I have served as a member of the IRC's Information Technology Committee (ITC) alongside senior IT executives from each of the ISO/RTOs. The ITC shares expertise and advice on existing IT functions and current activities within the wholesale electric industry and makes recommendations for IT standardization and architecture. The ITC has established a Security Working Group (SWG) to coordinate and communicate areas of mutual concern with regard to the development of applicable cyber and physical security practices. The SWG facilitates interactions among its members and collaborates to identify security issues and solutions.

Cybersecurity is a top priority throughout the industry, and the IRC is committed to collectively supporting the resiliency efforts of each ISO/RTO and advancing the cybersecurity posture of the power grid. Additionally, we have and will continue to partner with local, state, regional and federal governments, NERC, the Electric Sector Coordinating Council (ESCC), utilities and academia to stay ahead of the continuously advancing threats. Our core cybersecurity strategies focus on several key principles:

- Defense: Ensuring that we have the adequate controls and good security hygiene in place to prevent attacks.
- Response: Providing advanced security monitoring to correlate events and see patterns and indicators of compromise.

- Recovery: Maintaining continuity plans, exercises and drills to quickly recover critical systems in the event of a significant cyber event.
- Partnership: Coordinating with industry and government agencies before, during and after an event through the Electric Sector Coordinating Council (ESCC).
- Education: Recognizing the importance of every ISO/RTO employee in keeping the enterprise secure.

More than a decade ago the need for cybersecurity standards became evident as malicious activity was becoming more frequent and potentially destructive. Even with a dedicated collaborative focus on cybersecurity in the electric industry, standards were needed to address critical risks and ensure that all entities across the industry were appropriately protected and prepared. Developed by industry experts and facilitated by NERC, Version 1 of the Critical Infrastructure Protection (CIP) standards were approved by the Federal Energy Regulatory Commission (FERC) in 2008, making compliance with these standards mandatory and enforceable. Noncompliance could result in penalties as high as $1 million per day per violation.

Since first approved by FERC, the standards have been expanded to include all bulk electric system assets and their related cyber assets. Version 5 of the CIP standards became enforceable in July 2016 and consists of 11 different standards and approximately 110 sub-requirements for which we must each comply. These standards cover a wide range of risk areas from identification and classification of cyber assets to physical security, personnel and training, event monitoring, communication, incident response, protection and isolation of network architecture, access and change control, and system recovery. Though the CIP standards are continuing to evolve and mature to cover areas such as protecting our supply chain, the standards serve as robust, base-level requirements for securing our critical infrastructure. As an industry, we must maintain the flexibility and adaptability to implement the latest technological advances in securing our infrastructure. We must look beyond the standards as we secure the bulk electric system.

The IRC committees and working groups communicate and coordinate with organizations such as NERC's Electricity Information Sharing Analysis Center (E-ISAC) and local, state, regional and federal agencies, including the FBI and Homeland Security, to ensure that all ISO/RTOs are secure and prepared to act in a cyber emergency. Under the direction of NERC, coast-to-coast drills, referred to as Grid Ex, are conducted biannually to give all utilities opportunities to coordinate their response to simulated cyber and physical attacks on electric and other critical infrastructures across North America. Local, state, regional and federal government agencies, including the FBI and Homeland Security on the federal level and appropriate state and local agencies with which the ISO/RTOs closely coordinate on cybersecurity matters, as well as ISACs and supply chain organizations, are involved with the planning and execution of Grid Ex. Grid Ex IV is scheduled for this November. On a more frequent basis, individual ISO/RTOs are routinely involved in regional or statewide exercises conducted throughout North America, thus ensuring opportunities for organizations to verify their readiness to respond to and recover from cyber and physical attacks.

Though compliance with the CIP standards is mandatory and audited, with violations resulting in potential fines, the culture throughout the electric industry is maturing from one of compliance to a culture of security. A key element in the protection of our critical infrastructure is our implementation of multiple layers of security, known as a defense-in-depth strategy. While system redundancy is critical, ISO/RTOs also maintain close ties to the utilities they serve. If cyberattacks were successful on an individual ISO/RTO's critical infrastructure, neighboring

ISO/RTOs as well as member utility companies would immediately take action, assist with continuous operations and help isolate the attack to minimize any impact to the bulk electric system. Exercises such as Grid Ex give ISO/RTOs and their member utilities prime opportunities to practice their defense-in-depth strategies.

Additional developments in the electric utility industry to assist with resiliency include programs such as the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) which gives participating utilities early warning of potential cyberattacks. The ESCC has developed a Cyber Mutual Assistance (CMA) Program that provides emergency assistance, in the form of services, personnel or equipment, to participating entities in advance of, or in the event of, a disruption of electric service, systems or IT infrastructure due to a cyber emergency.

I speak on behalf of all of the ISO/RTOs in North America in stating that we are focused and committed to continuing to advance the security of the power grid and will continue to partner with local, state, regional and federal government agencies, NERC, the ESCC, utilities and academia to stay ahead of the continuously advancing and evolving threat. We must also remain involved in the development and implementation of regulations and standards to ensure that they allow for the flexibility needed to meet the security challenges we face in continuing to provide reliable, affordable electricity to consumers. It is essential that the electric industry continue to prioritize cybersecurity maturity above and beyond that which is required for compliance as the evolving threats and emerging technologies are surfacing faster than standards can be contemplated and promulgated. While the standards are indeed robust, we must not be complacent in our efforts to protect the bulk electric system from cyberattacks and must continue to maintain reliability and resiliency for the American people.