March 9, 2017

The Honorable Fred Upton
Chairman, Subcommittee on Energy
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Upton:

On behalf of the ISO/RTO Council, thank you again for inviting me to testify before the Energy Subcommittee at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." In response to the questions received on February 23, 2017, I have prepared the attached response. Please let me know if I can be of any further assistance related to this important subject.

Sincerely,

Barbara Sugg
Vice President of Information Technology, Chief Security Officer
Southwest Power Pool, Inc.
[redacted]

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

**The Honorable Morgan Griffith**

1. **Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.**

    a. **How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?**

    Instead of the industry receiving information individually from each of these agencies, a suggestion would be for the DOE, DHS and FBI to work directly with the E-ISAC to communicate threat information to the various entities. As the E-ISAC is governed by the E-ISAC Member Executive Committee of the ESCC which is the executive conduit between government agencies and the electric industry we believe that leveraging this existing governance model is an effective way to coordinate between government and industry. This is a similar model to the financial sector and communications sector.

2. **Some electricity utilities are participating in the Cyber Risk Information Sharing Program (CRISP), which allows the utilities to send network data for analysis against government sources.**

    a. **How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?**

    While CRISP is a valuable program, it is costly due to the fact that there are only a small number of participants and the entire cost of the program is shared amongst all of its participants. Subsidizing the cost for the government analysis, thus lowering the cost would encourage more entities to join. Please keep in mind that CRISP analysis is shared with the rest of the sector via the E-ISAC.

**The Honorable John Sarbanes**

1. **What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhanced or improved?**

    While the ISO/RTOs are not receiving direct federal funding support, we are partnering with DOE, DOD, the Defense Advanced Research Projects Agency (DARPA), and other research organizations who are receiving federal funding. In these cases we are providing industry expertise to guide research and development (R&D) investment. Additionally, the Electricity Subsector Coordinating Council R&D committee is working with government and industry focusing on high priority R&D topics: i) impacts of Electromagnetic Pulse (EMP) threats on the Power Grid, ii) enhanced communication capabilities during significant cyber or physical

disruptions, and iii) improved and automated threat information sharing across the electric sector and other critical infrastructure sectors, and iv) advanced automation capabilities to execute efficient response operations.

**The Honorable Jerry McNerney**

1. **The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the system, particularly cybersecurity, is a growing concern. Would you agree with this assessment?**

   The electric industry has a solid foundation of providing reliable electric service, but certainly the reliability, resiliency, and security of the bulk electric system must be taken into account. There is considerable ongoing discussion in various industry forums such as NERC and the Transmission Forum around resiliency and security, in addition to continuing discussion of traditional reliability issues. For instance, the industry is considering the disruption that can be caused by lower-frequency events (unusually severe weather, physical attacks, cyber threats, etc.) that have a potentially high impact on the electric system, often reflected in additional best practices that should be used in planning and operating systems.

2. **Is there a uniform definition used in the energy and electricity sector – or at the federal level – of what cyber "secure" or "resilient" means?**

   We do not believe there is a uniform definition that has been adopted within the electrical sector. However, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience attempts to define the terms as:

   Security - Reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

   Resilience - the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

3. **How costly is it to fund research RD&D from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel that cyber security and resilient investments are adequately reflected in rate-making cases?**

   Networks are typically designed in layers, which allow select areas to be upgraded and/or maintained without having a negative impact on other areas.

   Rate making-cases vary from region to region. Typically rate cases will not specifically identify security, but they implicitly include security requirements. Resilience is a broad term and the future will need to consider investment that improves upon traditional reliability and considers a grid with less critical components and resilience built into the design.

4. **Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?**

   ISO/RTOs operate at the wholesale level. Our "customers" are market participants, utility companies and transmission owners, therefore they are reasonably well versed in cybersecurity as they have standards they are required to meet.