

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Reliability Technical Conference

Docket No. AD19-13-000

**PREPARED STATEMENT OF NICK BROWN, PRESIDENT AND CHIEF EXECUTIVE
OFFICER, SOUTHWEST POWER POOL, INC.**

I. Introduction

I would like to thank the Federal Energy Regulatory Commission (FERC) for inviting me to participate in this Reliability Technical Conference. My name is Nick Brown, President and CEO of Southwest Power Pool, Inc. (SPP). SPP is one of seven FERC-designated regional transmission organizations (RTO) in the U.S. responsible for managing the electric grid, operating a wholesale electric market and planning transmission for all or part of 14 states, stretching from Louisiana to the Canadian border. We have been coordinating the flow of electricity in one form or another since 1941.

II. SPP Panel 1 Statement

Cybersecurity is a top priority throughout this industry, and the risk of cyberattack is SPP's top corporate risk. This is nothing new. For the past several years, SPP and the entire electric industry have worked to advance our collective resiliency efforts and the cybersecurity posture of the power grid through coordination with local, state, regional, and federal governments, NERC, the Regional Entities and many other organizations.

It is essential that the electric industry continue to prioritize cybersecurity maturity above and beyond that which is required for compliance, as evolving threats and emerging technologies develop faster than mandatory standards can be considered and promulgated. Perfunctory compliance with standards for the sake of clearing an audit is inefficient and ineffective. Instead, to ensure the reliability of the interconnected grid, our industry must collectively dedicate resources to meaningfully improve cybersecurity throughout the industry.

I have believed since the passage of the Energy Policy Act of 2005 that the transition to mandatory standards would be adolescently clumsy, and it has proven to be the case, largely

because the standards-development process is continually outpaced by technology and the scope, frequency and evolving vectors of cyber threats. Inconsistency in the interpretation of standards is another threat to security. SPP's most recent audit experience included the participation of four Regional Entities, FERC and NERC. At times, and reflective of regional distinctions, the auditors provided different input and varying interpretations of what it meant to be compliant. Credit is due NERC and the Regional Entities for their ongoing effort to harmonize real or perceived disparity among the Regional Entities. This effort should receive more priority though, so that it can actually bolster reliability by holding our industry to clear and uniform expectations and interpretations. After twelve years of mandatory standards, full maturity remains elusive in the cyber arena.

Evaluation by NERC and the Regional Entities of the effectiveness of standards should not be a pedantic exercise with unhelpful results. SPP participates in the NERC standards-drafting process to ensure the network architecture for its electronic security perimeter spanning multiple physical locations complies with CIP standards. Despite years of participation in this process and general agreement that this change is reasonable and secure, there is no end in sight for the drafting team's work. The pace at which security risks move and change dictate a limber review and determination of next steps. SPP encourages the Commission to ensure the standards review process becomes more efficient and responsive to the ever-changing landscape.

Standards should continuously be reviewed to determine needed modification, and how the standards are being enforced may be indicative of the need for refinement. Financial penalties associated with findings of noncompliance continue to increase, yet as the industry matures in its understanding of standards, the cyber-protections supporting the BES are stronger than ever. For example, enforcement entities should consistently distinguish between noncompliance and negligent security with respect to CIP standards. Penalties should be determined in light of needed investments in cybersecurity infrastructure and enhancements as part of the remedy for violating a requirement.

The SPP Regional Entity (RE) ceased operations in 2018. As President of the SPP RTO, I had no authority over the operations of the SPP RE. Yet, over the years, many of their registered entities approached me and not the SPP RE because they feared negative outcomes would result from seeking input directly from their Regional Entity. This is not healthy for reliability.

Whether or not there is a structural component to registered entities' reluctance to seek out input from their Regional Entities, there is much room for improvement in this space. Regional Entities should allocate resources to help registered entities fix gaps and operate in a compliant fashion without an inordinate focus on penalties. Additionally, enforcement proceedings are at times unbalanced and address first the items with the lowest impact on reliability. More difficult issues with potentially higher reliability impacts are left until the end of the process when, if the objective of these activities is the assurance of system reliability, they should be dealt with as quickly as possible.

As complementary to the vigor of enforcement proceedings, NERC and the Regional Entities should take full advantage of the outreach and assurance assessment component of the Risk-Based Compliance Monitoring and Enforcement Program (CMEP) to focus on issues that pose the higher risk to the reliability of the bulk power system (BPS). This collaborative approach encourages registered entities to establish robust internal controls that prevent, detect, and correct noncompliance and it allows the ERO to oversee and verify the activities resulting in the greatest benefit to reliability.

High-impact events such as gas-pipeline contingencies may be better addressed if the fuel supply chain were considered part of the BPS. Rather than leaving capacity obligations up to the regions, NERC could include them in its purview, thus bringing needed attention to the risks these types of contingencies pose to the BPS. This would enhance the long-term reliability of the system.

SPP collaborates regularly with NERC's Electricity Information Sharing Analysis Center (E-ISAC) to help ensure security and prepare for a cyber-emergency. The industry cannot afford to not participate in E-ISAC activities. However, actionable determinations by E-ISAC would improve the positions of those who participate. SPP supports elevating the strategic placement of E-ISAC within the industry in order to align industry's intelligence-collecting and analytical capabilities with the ever-increasing threats we face.

SPP is encouraged by the Commission's interest in the status of the ERO as demonstrated by this technical conference. Thank you for giving me the opportunity to share my thoughts on these important topics.