

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

**Security Investments for Energy
Infrastructure Technical Conference**

Docket No. AD19-12-000

**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 and the Department of Energy for inviting me to participate in the Technical Conference on Security Investments for Energy Infrastructure. My name is Nick Brown, President and CEO of Southwest Power Pool, Inc. (SPP). SPP is one of the seven FERC designated regional transmission organizations in the U.S, responsible for managing the electric grid, operating the wholesale electric market and planning transmission for all or part of 14 states, stretching from Louisiana to the Dakotas. We have been coordinating the flow of electricity in one form or another since 1941.

II. SPP Panel 2 Statement

Today, we continue to demonstrate the successful evolution of our organization, evidenced particularly by the maturation of our cybersecurity practices and the effective management of a grid that's increasingly proliferated with renewable generation sources. SPP acknowledges the risk of a cyberattack as one of our top corporate risks, and with the other North American ISO/RTOs, we support our collective resiliency efforts and the advancement of the cybersecurity posture of the power grid. We have and will continue to partner with state, local, regional, provincial and federal governments in Canada and the United States, NERC, the Electric Sector Coordinating Council, utilities and academia to stay ahead of continuously advancing threats.

Our core cybersecurity policies 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 SPP employee in keeping the enterprise secure.

In 2018, SPP selected an open-source cyber maturity model against which we could benchmark ourselves. We conducted a self-assessment and hired a consultant to perform an independent assessment using the same maturity model. The consultant also used a proprietary maturity and risk-assessment tool to evaluate SPP. Based on the resulting recommendations, staff prepared a strategic plan detailing five focus areas:

1. Standardized security architecture.
2. Supply-chain risk management.
3. Increased resiliency through focus on business continuity.
4. Further maturation of cyber best practices.
5. Expanded threat intelligence capabilities.

In late 2018, the Board of Directors and Members Committee accepted the staff report, acknowledged SPP's cybersecurity maturity and directed staff to execute the proposed cybersecurity goals over the next three years. These strategic goals will help SPP manage the ever-changing and significant threat of cyberattacks.

We and our peers are among the most highly regulated businesses in the U.S., subject to regulation and audits by FERC and are required to operate strictly under a FERC-approved tariff. We are likewise regulated and audited by the North American Electric Reliability Corporation (NERC), the reliability compliance enforcement authority. As part of the Energy Policy Act of 2005, NERC has the authority to fine electric utility entities more than \$1 million dollars per day per compliance violation.

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 FERC in 2008, making compliance with these standards mandatory and enforceable. Noncompliance could result in substantial penalties, as referenced above.

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 10 different standards and approximately 110 sub requirements to which we must 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.

It is essential that the electric industry continue to prioritize cybersecurity maturity above and beyond what is required for compliance as the evolving threats and emerging technologies are surfacing faster than standards can be contemplated and promulgated.

For example, SPP believes that it cannot deploy the required CIP controls for certain system information were it to be stored on externally-hosted servers (i.e., “the cloud”). Yet, we are finding that more and more vendors have flagship products that require all or a portion of CIP system information to be stored off-premises. This was a driving factor in our recent replacement of our service management software and has also been a complicating factor in the evaluation of vulnerability scanning and vulnerability management solutions. Hence, SPP has given weight to solutions that are more expensive or do not provide as much value as some cloud alternatives. The standards should not be so prescriptive as to force SPP to avoid industry trends that have proven to be secure, but not necessarily compliant.

In another example, SPP participates in the NERC standards drafting process to ensure that its network architecture for its electronic security perimeter spanning multiple physical locations is compliant 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.

It appears the financial penalties associated with findings of noncompliance are increasing, yet as the industry matures in its understanding of the standards, the cyber protections supporting the BES are stronger than ever. SPP appeals to the commission and DOE to ensure enforcement entities consistently make a distinction between noncompliance and negligent security with respect to the 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.

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, SPP also maintains close ties to the utilities we serve and the other ISO/RTOs. If cyberattacks were successful on an individual ISO/RTO's critical infrastructure, neighboring ISO/RTOs and 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 GridEx give SPP and other ISO/RTOs and their member utilities prime opportunities to practice their defense-in-depth strategies.

SPP collaborates with organizations including NERC's Electricity Information Sharing Analysis Center (E-ISAC) and local, state, regional, provincial and federal agencies in Canada and the United States, including Public Safety Canada, the FBI and Homeland Security, to ensure all ISOs/RTOs are secure and prepared to act in a cyber-emergency. NERC directs biennial coast-to-coast GridEx drills that give all utilities the opportunity to coordinate responses to simulated cyber and physical attacks on electric and other critical infrastructures across North America. On a more frequent basis, individual ISOs/RTOs are routinely involved in regional, provincial 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.

Additionally, SPP participates in several electric utility industry security programs such as the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) that gives participating utilities early warning of potential cyberattacks. SPP has engaged with entities such as the FBI, DHS with the Arkansas Fusion Center and the Kansas Intelligence Fusion Center to identify and evaluate potential threats to the bulk electric system. The ISO/RTO Council has a security working group on which SPP actively participates, to share and benchmark security practices among our peers. The Electricity Subsector Coordinating Council (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.

These programs require participant engagement to work effectively. More participation means clearer insight into actual and potential threats that will allow members to proactively reduce cyber and physical risk. Unfortunately, the time and resources needed to participate in these programs is potentially inhibitive. For that reason and to ensure real-time and accurate information sharing, centralizing cybersecurity information sharing should be considered.

The financial cost of some programs is high. CRISP, in particular, is a program that provides greater value as the number of participants increase, yet the cost of participating in the program is high and unaffordable for many smaller electric utilities. The first year of SPP's membership cost approximately \$300,000 then about \$180,000 per year thereafter. Since the total cost is divided between participants, the more participants, the lower the cost. There are also cost tiers based on network usage, and SPP is in one of the lower tiers of usage. Larger CRISP participants pay even more. The commission should encourage mechanisms to subsidize or otherwise make the program affordable for more utilities.

SPP's costs related to physical and cybersecurity are paid by our members and customers who then seek cost recovery from their respective state regulatory agencies as required in our FERC tariff. Cost recovery for our member utilities varies based on individual state regulatory agencies rate designs. For these reasons, I would encourage FERC to consider a joint technical conference between FERC, the Department of Energy and the National Association of Regulatory Utility Commissioners (NARUC) on this topic.

SPP fully supports and is encouraged by the Commission's interest in security investments in the energy infrastructure as demonstrated by this technical conference today. Thank you for giving me the opportunity to share my thoughts on this critically important topic.