UNITED STATES OF AMERICA

FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on Supply Chain Risk Management

Docket No. RM15-14-000

Prepared by Robert McClanahan

January 11, 2016

My name is Robert McClanahan, Vice President and Chief Information Officer at Arkansas Electric Cooperative Corporation (AECC). AECC is an electric generation and transmission cooperative in Arkansas that provides wholesale electricity to seventeen electric distribution cooperative members. These distribution cooperatives in turn provide electricity to approximately 500,000 retail members, primarily in Arkansas, covering just over 60% of the state's geographic area.

I would like to thank the Commission staff for the opportunity to provide testimony today concerning the important issue of Supply Chain Risk Management (SCRM). AECC believes that the risk associated with the supply chain should be analyzed from two broad perspectives: pre-implementation and post-implementation.

We believe that the post-implementation perspective, i.e., those risks to a system after it is under our operational control, is beyond the scope of today's proceeding and is sufficiently being addressed through company-specific cyber security programs based upon existing NERC CIP Standards. Our program's internal controls appropriately mitigate supply chain risks such as tampering, theft, unauthorized access and malicious software insertion.

The pre-implementation perspective, which includes risks such as manufacturing, software development practices, and counterfeit hardware and software, is far more difficult to control. AECC believes that this difficulty is a direct result of three primary factors. First, utilities the size of AECC do not have a large enough financial impact on vendors to control contractual terms related to Supply Chain Risk Management. As a result, we are often left in a position of accepting take-it-or-leave-it terms, with little or no ability to negotiate standard contractual provisions, much less pre-implementation supply chain risk controls. Even looking at the electric utility industry as a whole, AECC believes there is insufficient purchasing power for full control over the contractual terms of procurement.

Second, there are numerous supporting Information and Communication Technology (ICT) assets from multiple vendors that work together to make our control systems function. These include servers, networking equipment, storage and virtual infrastructure, and access control and monitoring systems. Even with proper supply chain risk management for power control systems, any risk assessment of the actual supply chain must factor in the supporting ICT assets. However, as discussed previously, utilities are often in no position to negotiate the contractual terms governing their procurement.

Lastly, vendors are not required to, nor do utilities the size of AECC have the means to, access, assess or audit supply chain vendors. The only tools available to utilities in this arena are assurances that a vendor provides through 3rd party assessments and certifications. However, these are often inconsistent in the controls tested and do not provide full assurance in the activities conducted during procurement.

Because of these three difficulties, as well as the regulation currently in place with NERC CIP, AECC encourages the Commission Staff to look toward non-punitive initiatives that encourage wider use of vendor certifications, along with research into technologies to assist in detecting and preventing fraudulent hardware. AECC asserts that the industry resource investment would be significantly more effective in these activities, rather than in new compliance initiatives.

In conclusion, AECC recognizes that managing supply chain risk is a vital part of any cyber security program and appreciates the Commission Staff highlighting the importance of this issue. This is a challenge that needs additional near-term research and testing. We have confidence that the FERC and industry will continue working together to support initiatives addressing cyber security risk in the supply chain.

Thank you.