UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management

Prepared Statement of Alberto Ruocco, Vice President and Chief Information Officer American Electric Power

Good afternoon members of the Commission Staff. My name is Alberto Ruocco. I am a Vice President and the Chief Information Officer at American Electric Power ("AEP"). I am the Co-chair of the EEI CIO group and Chair of the EPRI CIO group. I am here today representing AEP. I appreciate the opportunity to participate in this panel to address the important subject of supply chain risk management.

AEP is one of the largest electric utilities in the United States, delivering electricity to more than 5.3 million customers in 11 states. AEP ranks among the nation's largest generators of electricity, owning nearly 32,000 megawatts of generating capacity in the U.S. AEP also owns the nation's largest electricity transmission system, a more than 40,000-mile network. AEP's transmission system directly or indirectly serves about 10 percent of the electricity demand in the Eastern Interconnection and approximately 11 percent of the electricity demand in ERCOT.

AEP recognizes the significant risk inherent in our supply chain for cybersecurity-related risks; however, we recommend against a mandatory Reliability Standard for three reasons: 1) FERC jurisdiction limitations – that is, FERC cannot mandate supplier compliance (nor are suppliers likely to share competitive supply chain information), 2) the impracticality of managing to a standard over thousands of assets, each with a dynamic, multiple tier global

supply chain, and each subject to on-going potential design and implementation changes, and 3) NERC CIP v5 provides for supply chain risk management controls for the bulk electric system (BES).

For these reasons, AEP supports the voluntary development of guidelines through industry groups rather than a FERC-mandated Reliability Standard. For example, EEI collaborated with NEMA to distribute the *"Guideline Document – Supply Chain Best Practices"* (for electrical component manufacturers). These good practices identify five cyber security threat areas and recommend mitigation activities for manufacturers (in many cases with references to additional guidelines from ISO, NIST, IEC, etc.). In the third quarter of 2015, EEI published *"Principles and Resources for Managing Supply Chain Cybersecurity Risk"*. These five principles guide the electric utility to good supplier cyber security risk management practices (including additional resources from DoE, NIST, etc.). These guidelines are great examples of industry collaboration that provide relevant and practical guidance. If all these guidelines and principles fail to identify malware, NERC CIP Requirement 007 and cyber security best practices recommend building defenses in layers (a practice known as 'defense in depth') and current technology allows for continuous monitoring of all inbound, outbound and intra-company information communication. Malware will generate anomalous information communication that is likely to be identified by multiple monitoring tools through many layers.

AEP uses these publications, other voluntary guidelines, and emerging third-party assessments, methods, and practices to effectively manage grid reliability risks related to the cyber security of the supply chain. For other electric utilities that are unable to adopt all the best practices, the NERC CIP v5 requirements already address BES-related supply chain risk

management. Ultimately, suppliers that prove to be the most reliable and secure will emerge through competitive market forces – and these suppliers will be available to all electric utilities.

AEP has been a frequent contributor to the development of industry best practices in other disciplines working with peers, government agencies and other third parties. We are voracious consumers of good ideas from all potential sources including academic institutions, and other industries and subject matter experts (including suppliers). As a result, AEP has built its supply chain risk management program on the foundation of an assessment method developed over ten years ago through a collaboration of the Financial Services and Accounting industries. This method has a broad scope that applies to power systems components and related industrial controls and AEP uses it for all supply chain cyber-security related questions. As more companies adopt comprehensive supply chain risk management programs, and more suppliers are subjected to the scrutiny dictated by the assessment tools, industry best practices will evolve and improve – and AEP will benefit from continuous cyber-security risk reduction.

At AEP, we prioritize our supplier list and have evaluated hundreds of critical suppliers with our assessment tools. In each case, we determine the potential supplier risk based on over 1600 questions in eight categories. If necessary, we perform site visits to learn more and verify suppliers' answers.

AEP can continue to collaborate voluntarily with other electric utilities, EEI, and manufacturers to develop a uniform best practice for enterprise supply chain risk management assessments. Voluntary collaboration to define a uniform practice would move both the industry and its suppliers toward improved cyber security at lower overall costs to customers than through a new, incremental, mandated risk management Reliability Standard.

Another proposal is the development and implementation of an independent, third party cyber security assessment lab that tests and verifies BES-critical products from common suppliers. This shared lab resource would eliminate the need for each company to perform selected testing, which would help utilities more efficiently meet their existing NERC CIP cyber security requirements.

Given the complexities of any one vendor's supply chain and the unique characteristics of each utility, a Reliability Standard is likely to create inefficient and costly programs that may actually unnecessarily constrain a utility's supply chain cyber-security risk management program. In the end, each utility's supplier base is different so each utility will need the flexibility to manage their supply chain risk in a manner best suited to their scale, scope, complexity, resources and risk profile.