

AD19-12-000

**FERC Technical Conference on Security Investments for Energy Infrastructure
Introductory Comments of Nicholas Akins, American Electric Power**

Chairman Chatterjee, Commissioners and colleagues, thank you for the opportunity to participate in this important dialogue. My name is Nicholas Akins and I am the Chairman, President and Chief Executive Officer of American Electric Power (AEP). As one of the largest electric utilities in the United States, American Electric Power (AEP) is uniquely positioned to share our insights into the security risks and relevant reliability and resilience issues facing the grid today.

At AEP, we firmly believe that resilience begins with security, and security is resilience. Whether we are discussing cyber or physical security, I want to underscore two main points.

First, the threats we face are dynamic. At a minimum, we need to mitigate the changing environment by being able to check and adjust to threats as circumstances warrant. What exists today will be superseded by a new threat tomorrow. We need to stay ahead of this shifting landscape by proactively identifying threats and strategizing against them before they occur.

We can accomplish this through many tactics already in place. Current Critical Infrastructure Protection (CIP) Standards established by the North American Electric Reliability Corporation (NERC) form a firm foundation that allows each utility the opportunity to weave a set of solutions and protections that works best for their unique circumstances, including grid specifications, geography and a host of other variables.

Our mutual assistance efforts – once confined to storm recovery – have grown. We engage in spare parts sharing through programs such as Grid Assurance. This consortium will drastically eliminate resilience delays by ensuring that difficult replacement technologies – those large assets that often are

manufactured overseas – are already on hand and ready to be deployed when and where they are needed.

By definition, resilience is the ability of the grid to withstand and recover from events more quickly. Resilient design and material utilization – the manner in which we physically design the electric system – makes a difference. Enhanced real-time asset monitoring and extensive supervisory control and data acquisition (SCADA) make a difference. We have – and use – the ability to share these strategies and best practices with our peers. Our cyber security mutual assistance has grown to match our physical mutual assistance. NERC’s Grid Security Exercise (GridEx), the Electric Subsector Coordinating Council (ESCC) and the National Infrastructure Advisory Council ensure that we all are on the same page.

Transparent engagement with our federal and state lawmakers and regulators is critical, as is the implementation of protections to safeguard information that could provide a roadmap to those who would do us harm. As part of AEP’s regular meetings with our regulators, we do not leave behind information. There are no PowerPoints highlighting our most confidential strategies. No notes are taken in the meetings and transcriptions are not available. We also will not forward advanced copies of our talking points on sensitive security issues. This certainly is no reflection on our regulators. We trust them implicitly.

Nevertheless, any system can be hacked. While we would like to believe differently, the unfortunate reality is that nation-state actors and even lone-wolf terrorists can develop the capability to access utility and commission information networks. If commissions maintain extensive security details provided by utilities, an attack on a single network could compromise details that could be used against many utilities, not just one.

Our primary concern is protecting the confidentiality and security of our grid. Again, our industry is committed to engagement and transparency. However, I would be remiss if I did not point out the rising risk of Freedom of Information Act requests of those reliability organizations that govern us. Not unlike military briefings, what should be provided to the public and how it is provided is likely very different from what can and should be provided to those with the appropriate security clearances.

My second point is that regardless of what we do to protect our own systems, we each are as strong as our weakest interconnected peer. We must have unification between systems, regardless of who owns or controls those systems. Through the ESCC and other efforts, we already are talking and coordinating, sharing best practices. We need to continue such efforts and make sure everybody who should be in the room is in the room. The public-private partnerships we maintain are critical to the protection of our grid. We need to continue along our current path to strengthen both our security and our resilience.

Finally, transmission is the backbone of a secure grid. As such, we recommend an approach whereby FERC evaluates transmission owners' specific plans and actions, and awards an incentive based on their effectiveness in achieving stated resilience goals. AEP supports the Commission's intent to consider this vital topic.

In conclusion, AEP believes the risks we discuss here today are a matter of national defense. Whether we are discussing attacks intentionally perpetrated by a nation-state or the damages caused by natural disasters, any event that would weaken the grid would jeopardize national security.

Beyond the philosophical considerations, we need to remember that the grid does not stop at the borders of each state, each NERC region, or even international boundaries. For companies like AEP – and many others – a separate set of requirements for each jurisdiction is not just cumbersome, it potentially

could be counter-productive. We need consistency in a unified, risk-based approach from coast to coast. We need a risk based approach to security and therefore to resilience.

We must be laser-focused on those challenges that could result in the greatest risk to the grid and therefore to national security. We must work together in public-private partnerships to share best practices and refine those practices. We need to clear away the clutter and noise of efforts that do not serve a risk-based approach.

Thank you for your time today. I welcome questions and look forward to the coming dialogue. I appreciate the opportunity to participate in this critical conversation.