

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

Security Investments for Energy )                      Docket No. AD19-12-000  
Infrastructure Technical Conference )

**Written Statement of Kevin G. Wailes  
Lincoln Electric System**

**Panel II: Incentives and Cost Recovery for Security Investments**

My name is Kevin Wailes, and I am Chief Executive Officer of Lincoln Electric System, or LES, in Lincoln, Nebraska. I am also privileged to serve as one of the Co-Chairs of the Electricity Subsector Coordinating Council (ESCC). I commend the Department and the Commission for convening this conference to consider how the industry and federal and state authorities can work to promote energy infrastructure security, and I appreciate the opportunity to share my perspective on these important issues.

LES is a vertically integrated municipal electric utility serving approximately 140,000 customers in Lincoln and surrounding communities. We are a Transmission Owner member of the Southwest Power Pool (SPP). LES is a relatively large public power utility, but we are smaller than most investor-owned utilities, and most of the nation’s 2,000 public power utilities are smaller than LES.

I look forward to discussing all the issues raised in the Commission’s technical conference notice. In this statement, I focus on three topics. First, I will briefly describe the way public power utilities, including LES, recover their costs, in order to provide context for the broader cost recovery discussion on the agenda today. Second, I would like to discuss the proposition that access to reliable threat information and mitigation

strategies through the work of the ESCC and other government and industry venues facilitates prudent investment and reasonable cost recovery. Finally, I will highlight some areas where I believe targeted government support for industry initiatives can effectively promote infrastructure security, while also describing my concerns with the concept of using rate incentives to encourage cyber and physical security investment.

## **I. Public Power Cost Recovery**

Today's panel addresses cost recovery and incentives. As context for that discussion, I think it would be useful for me to start with a few observations about cost recovery by public power utilities.

With limited exceptions, public power utilities are not subject to state public service commission rate jurisdiction. Public power utilities are also generally excluded from the Commission's rate jurisdiction under the Federal Power Act, although some public power utilities, including LES, recover transmission revenues through RTO or ISO rates.

Rates for public power utilities generally are set by citizen-controlled boards or city councils. In the case of LES, for example, we are governed by an administrative Board consisting of nine members who are nominated by the mayor of Lincoln and confirmed by the Lincoln City Council. LES' rates are designed by LES staff using cost of service principles. The rates are adopted by the Board after a public hearing and then recommended to the Lincoln City Council, which has exclusive jurisdiction for establishing rates for LES' retail customers.

Many public power utilities, inside and outside of RTOs and ISOs, take wholesale transmission service and purchase wholesale power from public utilities. So when we

talk about cost recovery and incentives, it is important to keep in mind that public power utilities and the customers they serve may be paying these costs. And these costs may be on top of infrastructure security costs incurred by public power utilities on their own systems.

Public power utilities as a group maintain a healthy financial profile, and the ability and demonstrated willingness to adjust rates to recover necessary expenses has been recognized as a strength of the public power business model. At the same time, public power utilities like LES are directly answerable to the communities they serve and must remain mindful that there are limits to the costs that they can reasonably ask the members of their communities to bear.

## **II. Reliable Threat Information and Mitigation Can Promote Prudent Infrastructure Security Investment**

In considering investments to promote physical and cyber security, public power utilities, like other electric utilities, must weigh the security risks to utility infrastructure against the potential cost constraints on investments that might mitigate those risks and the adverse effects should an incident occur. A key component in striking the proper balance is having dependable information and awareness concerning the threats that the industry faces and informed approaches to mitigate these threats. In other words, access to reliable threat information and mitigation strategies can promote appropriate investment and adoption of best practices for cyber and physical security. This, in turn, can provide reassurance to regulators and utility customers that costs are being prudently-incurred and that rates reflect the reasonable costs of providing safe and reliable service.

There are a number of industry venues for utilities to share information and develop best practices, including the E-ISAC. As an ESCC Co-Chair, I would like to

highlight the role the ESCC plays in facilitating information sharing, cross-sector coordination, and planning for resilience, response, and recovery.

The ESCC is led by 30 utility and trade association CEOs, and it serves as the primary liaison and information exchange platform between utility senior leadership and senior members of the federal government.

A principal area of focus for the ESCC is coordinating with the federal government, and with other interdependent critical infrastructure sectors to improve major incident planning and response. Priority efforts include working with industry and government stakeholders, along with vendors, to identify and share best practices to address threats to the supply chain. Ongoing ESCC-supported R&D includes coordination of industry and government efforts to enable the development and implementation of resilient emergency communications capabilities.

The ESCC also works with the government and the private sector to improve information sharing capabilities, tools, and technologies. The ESCC, for example, participates in classified government briefings, and is able to use the actionable intelligence from such meetings to bolster cyber and physical security of the industry through the Electricity Information Sharing and Analysis Center (E-ISAC). And the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership that the Department helps fund in conjunction with the E-ISAC, facilitates mutual sharing of actionable threat information. CRISP utilizes advanced tools to identify threat patterns and trends across the electric power industry.

A third focus area of the ESCC is enhancing resilience, response, and recovery efforts in the event of an incident. The GridEx exercises hosted by NERC, for example,

are powerful tools for the industry to assess readiness for catastrophic events. The ESCC and our federal government partners participate in the exercises and use the “lessons learned” to develop solutions to problems identified during the events. The lessons from GridEx III in 2015, as well as the Ukrainian cyber incident prompted ESCC to focus on potential supplemental operating strategies that would allow the grid to continue to operate in a sub-optimal state.

The ESCC’s four strategic committees (Threat Information Sharing; Industry-Government Coordination; Research & Development; and Cross-Sector Liaisons) also facilitate collaboration between government and industry technical experts. The work done by these committees is translated into products and systems that benefit industry and government and assist in the development of the utility industry’s culture of cyber preparedness.

Facilitating access to reliable threat awareness information through the ESCC and other programs can inform appropriate investment and adoption of best practices for cyber and physical security by public power utilities. In my experience, public power utilities are willing to make necessary, risk-appropriate investments to promote infrastructure security, and the local rate-setting process used by most public power utilities allows them to support these investments.

### **III. Financial Incentives and Special Cost Recovery Mechanisms**

I believe there can be a role for state and federal government to play in supporting utility investment in infrastructure security in certain contexts. In general, however, I don’t believe there is a need to use rate incentives or special cost recovery mechanisms to promote investments in physical and cyber security.

The technical conference notice asks about the availability of grants for industry to assist with security investments. In my experience, relatively small investments by the government can pay big dividends in promoting infrastructure security, even where the dollars are not spent on specific facilities. As an example, in 2016 the American Public Power Association (APPA) entered into a three-year cooperative agreement with DOE that provides APPA with funding to help public power utilities create stronger, more secure cyber systems. The program has developed a self-assessment tool, or scorecard, based on DOE's Electricity Subsector Cybersecurity Capability Maturity Model, or C2M2, that gives utilities a starting point to address cyber risks. The program is also currently working to create a cybersecurity program roadmap, which will provide specific strategies and guidance for a number of key areas. Under this program, public power utilities can also receive funding and support to implement technology to improve their cybersecurity posture. This program is particularly valuable for small public power utilities.

I cite the DOE-APPA cooperative agreement as an instance where, in my view, targeted support for industry initiatives has really moved the needle in promoting infrastructure security. The case for ratemaking incentives or special cost recovery mechanisms to encourage and prioritize infrastructure investments is much less compelling.

Public utilities should not receive incentives for security investments that they are already obligated to make, such as the costs associated with NERC reliability standards compliance. Many of the grid security costs we are talking about are likely to be recoverable, with a rate of return, in cost-based transmission rates regulated by the

Commission or in retail rates subject to state jurisdiction. This cost-based recovery should in most cases be sufficient to support prudent infrastructure security investment. In the case of competitive generators that recover their costs through market-based rates, ensuring security is a cost of doing business in the market that can be recovered through contracts or market bids. It is difficult for me to see why customers of utilities like LES should be asked to subsidize that one particular cost of doing business for competitive suppliers. Public power utilities should not be asked to pay more to incent prudent investment by public utilities, particularly when these additional costs may be on top of infrastructure security costs incurred by public power utilities on their own systems.

Speaking from my own experience, I don't view a lack of rate incentives as a limiting factor on the industry's willingness to make prudent infrastructure investments. Public utilities already have numerous financial, legal, and reputational incentives to promote physical and cybersecurity. While the regulatory process can present a certain amount of cost recovery risk, the best way to address that concern is, to reiterate my earlier remarks, by facilitating information sharing about the risks that utilities face and prudent approaches to mitigate those risks. I would also be concerned that rate incentives could influence utilities to focus on infrastructure investments that are eligible for incentives, which might not necessarily be the soundest risk mitigation or recovery approach in a given situation.

Finally, section 215A of the Federal Power Act includes specific provisions addressing recovery of costs incurred in connection with declared grid security emergencies, which can include physical and cyber-attacks, as well as disruptions caused

by a geomagnetic storm or electromagnetic pulse.<sup>1</sup> In considering other mechanisms for the recovery of infrastructure security-related costs, the Commission would need to address how any such mechanisms are consistent with Congress' provision of specific, limited authority to recover certain costs incurred in responding to grid emergencies.

#### **IV. Conclusion**

I appreciate the opportunity to provide this written statement for the record, and I look forward to discussing these and other issues at the technical conference.

Dated: March 26, 2019

---

<sup>1</sup> 16 U.S.C. § 824o-1.