UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference	)	Docket No. AD18-11-000

Statement of Paul Crist
Vice President, Technology Services & Chief Technology Officer,
Lincoln Electric System

July 31, 2018 Reliability Technical Conference

Panel IV: Addressing the Evolving Cybersecurity Threat

Good Afternoon, I am Paul Crist, the Chief Technology Officer and Vice President of Technology Services for the Lincoln Electric System, referred to as LES, in Lincoln Nebraska and I appreciate the opportunity to provide these comments. LES is a vertically integrated municipal electric utility serving 140,000 customers in Lincoln and surrounding communities. LES owns and operates transmission, distribution and generation in its footprint, has joint ownership of generation in Wyoming and Iowa, and has power supply purchase agreements from plants in Nebraska, Kansas, Oklahoma and South Dakota. LES is also a member of the Southwest Power Pool (SPP), Midwest Reliability Organization (MRO) and is registered in seven categories of NERC Functional Entities.

In addition to having a proactive cybersecurity program and integrated "operating technology" and "information technology" staff, LES believes that it is critical to be actively engaged in the industry efforts to maintain grid security. In support of that philosophy, I have served on the NERC Critical Infrastructure Protection Committee (CIPC) for almost 10 years, including chair of the Compliance Input Working Group and the LES CEO, Kevin Wailes, is a co-chair of Electricity Subsector Coordinating Council (ESCC) which leverages the capabilities of the Department of Energy (DOE), Department of Homeland Security (DHS) and many other government agencies with the electric utility industry.

LES was one of the utilities that received a FERC-led NERC CIP Audit. The audit was not only a review of our compliance with the NERC CIP Standards, but provided a productive two-way discussion around cybersecurity. These types of discussions are very beneficial to allow the industry to move forward outside the auspice of mandatory standards that can create challenges when applying new advanced technology. I agree that the evolving cybersecurity threat is a key area of focus for the Commission and it needs to be addressed with the proper approach. It is important to emphasize that electric utilities are very cognizant of cyber threats and vulnerabilities, and utilities are continually identifying new and improved ways to mitigate and prevent cyber threats, but we need to be allowed certain flexibility to change technologies quickly to respond to the rapidly changing threat environment.

Utilities are continually improving their security postures to mitigate emerging threats and vulnerabilities based on risk. Utilities with critical infrastructure assets are very good about sharing information and continue to develop different approaches to sharing information. Most of the regions have technical groups that meet routinely to address emerging threats and to share ideas around mitigating those threats. The information sharing involves how to remain compliant while approaching new threats with innovative approaches. The NERC CIP Standards have forced discussions between the regulators and asset owners and operators, but due to the enforceable nature of the standards, compliance discussions have dominated the discussions during audits and not provided an avenue for information sharing and improving our overall cybersecurity posture. The focus on the compliance and evidence creation is important, but it often consumes a valuable amount of time from industry cybersecurity subject matter experts which has the effect of impeding focus and attention on dynamic emerging threats.

Risk Mitigation is best accomplished through flexible programs and options outside of NERC standards that can enhance cybersecurity and provide all utilities with actionable options, no matter how big or small. Utilities, industry groups, and associations are continually developing, identifying, and

sharing best practices. LES, as well as many other utilities, participate in activities to help develop and share ideas on approaches to mitigate threats. These activities involve discussions around applying technology and best practices, including addressing the human factor in mitigating these threats. Utilities are utilizing guidelines and best practices developed by NIST and DOE OE to include procurement language in contracts addressing cybersecurity for industrial control systems. Cybersecurity involves multiple approaches and any one solution is not adequate and it requires constantly changing technology and approaches.

Another example from the public power sphere I would like to highlight is the American Public Power Association's (APPA) Cooperative Agreement with DOE that has helped develop a right-sized approach to determining a utility's cybersecurity maturity. The DOE's Electricity Sector Cybersecurity Capability Maturity Model (ES-C2M2) allows utilities of all sizes to develop a score that can be used to compare to other utilities and to focus their efforts to improve their cybersecurity defenses. LES has recently completed our annual assessment to allow us to focus our efforts where we need to improve and mitigate our risks. We received our training through APPA as part of the APPA contract with four training organizations. Training is essential to ensure the public power workforce, and all utilities, to understand the risk and to take the appropriate action to further enhance their cybersecurity maturity level.

LES, and other public and private utilities, support the enhancement of the Electricity – Information Sharing and Analysis Center (E-ISAC) and the work that is being done with the ESCC and the government partners to improve information sharing. The engagement with the ESCC Members Executive Committee provides appropriate priorities that utilities need. The CRISP program is an example of industry-government information sharing to identify emerging threats. The recently developed Industry Augmentation Program to support utility subject matter experts embedded in the E-ISAC began this year and has received positive feedback from both E-ISAC staff and utility staff. Through

various outreach efforts, the electric industry has dramatically increased information sharing among regions and government agencies. The NERC CIPC is another example of a forum that brings industry physical, cyber, and operational experts from the seven different regions together to share best practices and to develop security guidelines, outside of any mandatory standards. There are also numerous industry groups such as the North American Transmission Forum (NATF) and North American Generator Forum (NAGF) that provide additional venues for utilities to share and develop best practices.

Information sharing between government and industry about current and emerging threats is critical to protecting the electric grid. Information sharing is improved when there is not a fear of retribution for sharing information. To continue to improve information sharing, there needs to be a clear separation between those working to improve the security posture of industry and those involved in mandating or enforcing regulations. If regulations are going to be mandated, they need to be a flexible framework to protect against the threats of tomorrow and not just the threats of today. The maturation of the ESCC which provides the collaboration of industry and the various government partners is the best forum for that engagement. The ESCC collaboration best avoids potential duplication of different Agency efforts. Additionally, the relationship avoids the potential for competing regulations from different agencies. The ESCC focuses on the policy level and allows the utilities to focus on operational challenges with government partners. As part of this ongoing collaboration between the industry and our government partners, the protection of Critical Energy Infrastructure Information (CEII) is a crucial part of mitigating attacks against our infrastructure and all agencies need to protect this information.

Emerging technology can present new vulnerabilities but also new opportunities and efficiencies. Cloud computing is an example of a newer technology that wasn't considered with the current NERC CIP Standards and is proving challenging for our industry to leverage. Cloud computing is a paradigm-shifting technology for the electric industry and other industries. With the increasing

amount of data that comes with grid modernization, the cloud provides a terrific opportunity to leverage the advanced analytics and capabilities to improve the resiliency and efficiency of the grid. The cloud can be utilized to take advantage of the advanced security analytics to mitigate threats against the grid and is available to utilities of all sizes. The cloud provides an opportunity to improve the resiliency of systems by providing another opportunity for recovery from a cyber or physical incident.

To allow utilities to consider using the cloud, a sub-group from the NERC CIPC called the Compliance Input Working Group is developing a framework within the CIP standards to be able to utilize cloud technologies. The group is working with industry subject matter experts in cyber and physical security, as well as, several large vendors to develop implementation guidance that will hopefully meet the requirements of the NERC CIP standards. As stated earlier, industry is very cognizant of cyber threats and we want to make sure any new technology, such as cloud computing, provides the protections necessary to meet our concerns. The data and systems that are placed in the cloud need to be protected at the same level, or higher, than that of on-premise solutions.

As stated earlier, LES was one of the utilities that received a FERC-led audit. We have also been engaged with FERC staff in exploring options around application whitelisting to improve industry's security posture and incident response. These engagements with FERC provide an open discussion and information-sharing between FERC and industry and provide a great partnership to address the emerging threats. The constantly changing cyber threats are difficult to mitigate with one-size-fits-all standards, and sometimes the standards can prove challenging to industry due to the lack of flexibility or adaptability. To best improve our capabilities, it comes down to people and tools to fit the appropriate needs of the industrial control system. The ESCC's Cyber Mutual Assistance Program is an example where industry has developed a process for mutual assistance between utilities during major cyber events. Regardless of technology, a robust, flexible, and layered approach to security and incident response is needed.

When considering the emerging cyber threats to industrial control systems, the voluntary development, application, and sharing of best practices must be utilized to improve the cybersecurity capabilities. The current NERC CIP standards are challenging for utilities when emerging cyber threats are discovered and ultimately put the utility in a situation of having to choose between being compliant and being secure. An example of this occurred when there was a concern about certain software being malicious and this same software was being used in industrial control systems to meet the malware protection requirements of the CIP standards. Utilities had to choose between removing the software and not meeting the CIP requirements, or keeping the software in place to be compliant and trying to mitigate the risk of the software through other means. As utilities continue to hone their cybersecurity capabilities with industrial control systems, the sharing of best practices is critical and provides another opportunity to mitigate the cybersecurity risks associated with emerging threats.

The current NERC CIP Standards have consumed a tremendous amount of valuable industry time on development and modifications to the standards. The CIP Standards continue to evolve to address new threats and shortcomings of the existing standards. The constant modification to the standards creates a lot of frustration with subject matter experts when they are required to continually monitor for changing compliance requirements instead of looking for emerging threats. The NERC CIP standards provide an opportunity for utilities to focus their efforts on building up their cybersecurity defenses, but as the threats and technology rapidly change, the standards become quickly outdated and an impediment to moving forward. We do not need to have a standard to address every new threat and technology, but rather a more robust framework that provides flexibility to adapt quickly without needing to decide between being compliant or being secure.

Conclusion

I want to thank you again for this opportunity to provide this written statement for the record. I look forward to having a conversation about these critical issues at the technical conference.