CELEBRATING 30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

April 11, 2017

The Honorable Cory Gardner
Chairman, Subcommittee on Energy
Committee on Energy and Natural Resources
304 Dirksen Senate Office Building
Washington, D.C. 20515

The Honorable Joe Manchin
Ranking Member, Subcommittee on Energy
Committee on Energy and Natural Resources
304 Dirksen Senate Office Building
Washington, D.C. 20515

Dear Subcommittee Chairman Gardner and Subcommittee Ranking Member Manchin,

On behalf of the Large Public Power Council, thank you for the opportunity to testify at the Senate Energy and Natural Resources Subcommittee on Energy's hearing on March 28th regarding industry efforts to engage on cyber security. Per your request, we are providing the following comments for the record in response to questions posed during and following the hearing.

During the hearing Subcommittee Chairman Gardner asked how to engage more utilities in the Electricity Subsector Coordinating Council's (ESCC) Cyber Mutual Assistance (CMA) Program. I would like to provide for the record the following information gathered by the Edison Electric Institute:

> CMA participating utilities are serving approximately 80% of all US electricity customers. By counting utilities that serve customers within the United States, and excluding Independent System Operators (ISOs), Regional Transmission Organizations (RTOs) and Canadian entities, EEI determined that there are over 118 million customers represented by utilities that participate in CMA. In fact, the impact and reach of CMA is significantly higher than that, given the level of participation by ISOs and RTOs who do not directly serve end-use customers.

We believe the CMA provides significant value to utilities and their customers, and we support efforts to engage utilities in this voluntary program.

Following the hearing, citing attacks in California and Arkansas, Subcommittee Ranking Member Manchin asked for our perspective on the seriousness of these attacks and, based on these experiences, what emerging technologies, if any, are primed to protect against physical attacks on the grid. The physical attacks to the grid in both California and Arkansas were cause for great concern. These attacks raised concerns to a heightened level due to their sophistication and potential for wide-spread damage.

For physical attacks, and more recently cyber attacks, the electric industry does have a well-developed and robust information sharing framework. Through tools like the North American Electric Reliability Corporation (NERC) Electricity Information Sharing and Analysis Center (E-ISAC) Portal and the Department of Homeland Security Critical Infrastructure sector program, grid operators share information with local, state and federal law enforcement as well as other industry

partners. Comprehensive post-incident analysis related to physical attacks has been conducted in order to raise vulnerability awareness and to prevent similar attacks. These analyses are shared, through a variety of industry forums.

The NERC Physical Security Reliability Standard (CIP-014-2) directed by the Federal Energy Regulatory Commission (FERC) in a March 7, 2014 Order requires the identification and protection of transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or cascading within an interconnection.

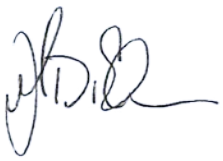
The purpose of the Standard is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System facilities against physical attacks. The Standard became effective in October 2015. Specific security practices and technologies were not prescribed by the Standard; however, assessments did focus on security strategies designed to detect, deter, delay and respond to incidents.

Most hardening involves a combination of enhanced physical barriers, such as larger walls preventing visibility into critical sites. Another common measure is controlling proximity and access through secondary perimeters and controls. Technology is also deployed to protect assets. Advanced intrusion detection systems, video surveillance cameras with thermal video and analytic capabilities are used regularly to enhance physical security. In some cases, increased security patrols or a physical security presence at the site are utilized. Some combinations of these techniques, along with increased coordination with law enforcement, serve to reduce the risks of physical attacks. Finally, many grid operators are building security into their system design protocols configuring or separating their systems to build redundancy.

Lastly, during the hearing witnesses were invited to provide additional feedback on S. 79, the Security Energy Infrastructure Act. We would like to echo comments made by Mr. Michael Bardee, Director of the Office of Electric Reliability at FERC, for the inclusion of FERC in the working group established by S. 79. We believe the studies set forth in S. 79 would benefit greatly by the inclusion of FERC.

Thank you again for the opportunity to testify, and we look forward to continued dialog on these critical issues.

Sincerely,



John Di Stasio
President
Large Public Power Council